Myndigheten för samhällsskydd och beredskap

Kan era kemikalier användas för terrorattacker?

En vägledning om att motverka terrorism och annan allvarlig brottslighet med kemiska produkter

Kan era kemikalier användas för terrorattacker?

Tryck: DanagårdLiTHO

Produktion: Advant

Publikationsnummer: MSB1426 - september 2019

ISBN: 978-91-7383-962-4

Förord

Syftet med denna vägledning är att försvåra, och i bästa fall förhindra, terrorism och annan allvarlig brottlighet med kemikalier och kemiska produkter. Händelser här hemma och i vår omvärld ger anledning till att öka medvetenheten kring problematiken och se över skyddet. Vägledningen har skrivits för att hjälpa berörda verksamheter att förbättra sitt skydd och riktar sig framför allt mot mindre verksamheter som inte själva har system för det. Omfattningen och metodiken är på en övergripande nivå och många av de åtgärder som kan förebygga händelser är förhållandevis enkla att genomföra.

I framtagandet av denna vägledning har ett antal representanter för näringslivet deltagit med konstruktiv kritik och goda idéer som avsevärt har förbättrat innehållet. Vägledningen baserar sig på ett 2:4 projekt lett av Totalförsvarets forskningsinstitut (FOI) som även varit behjälpliga i inledningsskedet av arbetet.

Detta är den första utgåvan av vägledningen, publicerad i september 2019.

Innehåll

Inledning 7

1. Övergripande systematik 8

2. Förberedelser 9
2.1 Utse en arbetsgrupp 9
2.2 Identifiera berörda kemiska produkter 9
2.3 Bedöm informationens skyddsvärde 10

3. Berörd infrastruktur och information 11
3.1 Identifiera berörd infrastruktur 11
3.2 Identifiera känslig information 11
3.3 Identifiera nyckelpersoner 11

4. Hotbild 12

5. Händelser och deras effekter 13
5.1 Utsläpp av kemikalier från verksamheten 13
5.2 Explosion eller brand i verksamheten 13
5.3 Utsläpp av kemikalier på andra platser 14
5.4 Explosioner på andra platser 14
5.5 Belastning på samhällets resurser och produktflöden 14
5.6 Fabricerade händelser ("fake news") 14

6. Orsaker till att en händelse inträffar 15
6.1 Angrepp på förvaringsställen 15
6.2 Fysiska ingrepp i processer 15
6.3 IT-angrepp 15
6.4 Stölder 16
6.5 Köp från obehöriga 16
6.6 Transporter utanför det egna området 16
6.7 Hot mot och utpressning av nyckelpersonal 16

7. Förebyggande barriärer 17
7.1 Fysiska barriärer 17
7.2 Organisatoriska barriärer 17
7.3 IT-säkerhet 18
7.4 Securitykultur – en medveten personal 18
7.5 Utbildning och övning av personal 19
7.6 Intern och extern kommunikation vid händelser – kommunikationsplan 19

8. Exempel på metod för att förbättra skyddet 20
8.1 Bow tie-analyser 20
8.2 Prioritera barriärerna och gör en handlingsplan 22

9. Omvärdera med jämna mellanrum och vid behov 23

Bilaga 1 – Berörda kemiska produkter 25
Kemiska produkter som har farliga egenskaper 25
Utgångsämnen (prekursorer) till explosiva
och mycket giftiga kemikalier 26
Övriga kemiska produkter 27

Bilaga 2 – Kortfattad hotbild 29

Inledning

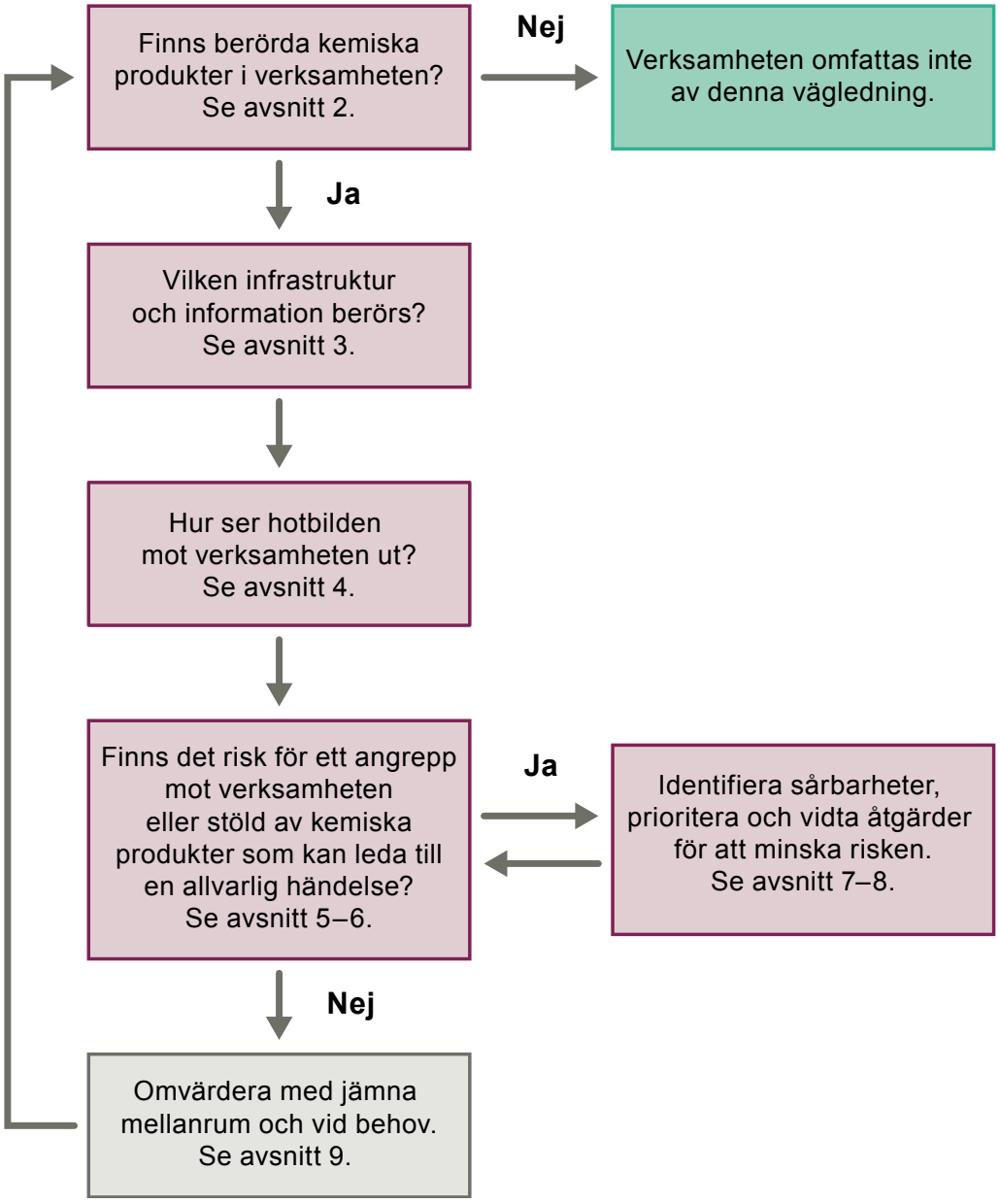
Om er verksamhet hanterar kemiska produkter med farliga egenskaper kan en terrorist eller annan brottsling vilja komma åt dem för att orsaka allvarlig skada. Det gäller även produkter som innehåller utgångsämnen (prekursorer) för att tillverka farliga ämnen. Denna vägledning innehåller en metodik som stöd för att förbättra skyddet i er verksamhet och förslag till åtgärder för att minska risken för en attack med kemiska produkter. Vägledningen riktar sig framför allt till mindre verksamheter som inte har egen expertis i denna typ av frågor och kanske inte ens upplever sig hantera kemiska produkter.

Terrorism och annan allvarlig brottslighet med kemikalier kan på flera sätt orsaka skada på både verksamheten och samhället. En kemisk industri kan utgöra ett mål i sig då ett sabotage kan få stora konsekvenser i form av utsläpp av skadliga ämnen, brand eller explosion i verksamheten. En distributör, lagerhållare, återförsäljare eller användare kan råka ut för stöld av kemiska produkter som kan användas för att orsaka skada på annan plats. Den skada som kan åstadkommas med kemikalier beror i viss utsträckning på mängden, men även mindre kvantiteter kan ge stor effekt beroende på kemikaliens egenskaper och den aktuella situationen. Vägledningen vänder sig därför till er som hanterar kemiska produkter i såväl större som mindre skala. Det finns även andra vägledningar inom området som kan vara till stöd.[1]

1. Se t.ex. CEFIC:s vägledning ”security code” inom säkerhetsprogrammet Responsible Care, www.cefic.org.

1. Övergripande systematik

Ett arbete för att förbättra skyddet mot terrorism och andra brottsliga handlingar är ett löpande arbete. I denna vägledning används systematiken som framgår av följande flödesschema:



2. Förberedelser

Innan ni påbörjar arbetet behöver ni först och främst reda ut om några berörda kemiska produkter hanteras inom verksamheten och i så fall vilka de är. Fundera också på vilka personer som behöver engageras i arbetet och hur ni ska ta hand om informationen som tas fram.

Finns det kemiska produkter i verksamheten som kan orsaka allvarlig skada?

2.1 Utse en arbetsgrupp

Arbetet med att förbättra och stärka skyddet mot terrorism och andra brottsliga handlingar bör vara förankrat hos chefer, företagsledning eller motsvarande och de bör också vara involverade i den grad arbetet och verksamheten kräver det. Förslagsvis gör ni arbetet i samverkan mellan säkerhetsansvariga, personal inom säkerhet-hälsa-miljö, skydds- eller arbetsmiljöombud och personer med kunskap om kemikalier. Det kan vara aktuellt att även blanda in personalavdelningen. Vilka och hur många personer som deltar beror i hög grad på verksamhetens storlek och typ, och behöver därför dimensioneras med hänsyn till detta. Den initala bedömningen att identifiera vilka berörda kemiska produkter som finns hos er verksamhet (se avsnitt 2.2) kan förslagsvis göras i en mindre grupp med kunskap och mandat för detta.

2.2 Identifiera berörda kemiska produkter

Att identifiera alla kemiska produkter som skulle kunna användas för att åstadkomma allvarlig skada är ett omfattande arbete som kräver expertkunskap.

Kemikalielista finns i **bilaga 1**

För att hjälpa verksamheter som inte har tillgång till sådan expertis har de farliga egenskaper som mest uppenbart kan användas för brottsliga handlingar listats i bilaga 1, tillsammans med information om hur produkterna märks. Bilaga 1 innehåller även hänvisning till ett antal specifika kemikalier som kan användas för att tillverka giftiga och explosiva ämnen, men som i sig själva inte behöver ha farliga egenskaper. Listan i bilaga 1 är inte uttömmande och generellt kan sägas att om ett ämne direkt eller indirekt kan orsaka en allvarlig olycka kan det förmodligen också användas för att skada med avsikt.

Tänk på att även blandningar omfattas om halten av aktuella ämnen är hög eller blandningen bara innehåller ett fåtal andra ämnen (så att aktuella ämnen skulle kunna utvinnas ur blandningen).

Om ni kommer fram till att ni har kemiska produkter som kan åstadkomma skada, fundera över om mängderna är relevanta. En liten flaska med aceton på laboratoriet eller verkstadsgolvet är exempelvis inte särskilt relevant med tanke på att aceton är mycket lättillgängligt i samhället.

Om ni kommer fram till att ni inte har några kemiska produkter som omfattas, berörs ni i nuläget inte av denna vägledning. Om verksamheten förändras och nya produkter tillkommer kan en ny utvärdering dock behöva göras.

2.3 Bedöm informationens skyddsvärde

Förutsatt att ni har en eller flera kemiska produkter som kan användas för att åstadkomma skada, behöver ni gå vidare med ert arbete och engarera arbetsgruppen (se avsnitt 2.1).

Börja med att bedöma i vilken utsträckning den information som ska hanteras i arbetsgruppen behöver skyddas. Vem ska ha tillgång till vilka delar av informationen? Behöver ni någon särskild typ av utrustning för att hantera känslig information (t.ex. ”stand-alone datorer” eller säkerhetsskåp). Fundera över vilken information som kan hanteras över osäkra nät (mejl, telefon, fikarummet, chat-appar, osv.), vilka som kommer att ta del av informationen (t.ex. anställda, konsulter och underleverantörer) och hur eventuella säkerhetskopior ska skyddas.

Se även **avsnitt 3.2**

Det kan vara aktuellt att dela upp den information som sammanställs i två delar – en öppen del som går att sprida och en konfidentiell del med mycket begränsad spridning. Utan att överdriva den typen av begränsningar är det betydelsefullt att reflektera över detta. Man talar i sammanhanget ofta om ”right to know” och ”need to know”, dvs. att känslig information endast delges dem som har både befogenhet och anledning att känna till den (se även avsnitt 3.2).

3. Berörd infrastruktur och information

För att förbättra skyddet av kemiska produkter behövs givetvis en analys om var de finns. Även känslig information om dem och vilka personer som har tillgång till denna behöver ingå i en sådan analys.

Var finns de kemiska produkterna?

Vem har tillgång till eller information om dem?

3.1 Identifiera berörd infrastruktur

Fundera kring var de berörda kemiska produkterna finns:

- Var förvaras de (förråd, cisterner, lastkajer, etc.)?
- Hur kommer produkterna till företaget/förrådet och hur lämnar de detta?
- I vilka rör och processer förekommer kemikalierna?
- Var finns styrsystem, pumpar, ventiler och andra anläggningsdelar för kemikalierna?

3.2 Identifiera känslig information

Finns känslig information inom organisationen och hur hanteras den i så fall? Känslig information är t.ex. uppgifter som skulle kunna underlätta stöld eller sabotage eller som gör det möjligt att kringgå verksamhetens säkerhetssystem. Det kan vara sådant som rör:

- Personalens befogenheter
- Anläggningsritningar, kemikalieförteckningar och processcheman
- Lagring och transporter av berörda kemiska produkter
- Lås, koder och övervakningsrutiner

Gör en kartläggning av hur känslig information bör skyddas med hänsyn till att den alltid ska finnas när den behövs (tillgänglighet), att den går att lita på och är korrekt (riktighet) och att den bara är tillgänglig för behöriga personer (konfidentialitet). Detta gäller både digital och pappersbaserad information, inklusive information som hanteras i industriella informations- och styrsystem, t.ex. ICS/SCADA[2]. Resultatet av kartläggningen bör hanteras som känslig information (se avsnitt 2.3).

Se även **avsnitt 2.3**

3.3 Identifiera nyckelpersoner

Nyckelpersoner är personer som har tillgång till avgörande information eller verktyg för att komma åt berörd infrastruktur eller känslig information. Det kan exempelvis vara säkerhetspersonal som har kontroll över inpasseringen till området, fabriksansvariga som har koder och nycklar eller IT-ansvariga med behörigheter och lösenord.

2. ICS står för Industrial Control Systems och SCADA står för Supervisory Control And Data Acquisition.

4. Hotbild

Även om det inte finns ett uttalat hot mot kemisk industri är verksamheten en potentiell måltavla för terrorism.

Terrorism är ett reellt hot mot Sverige enligt Nationellt centrum för terrorhotbedömning (NCT)[3], som är den instans som bedömer hotnivån i Sverige. Även om inget uttalat specifikt terrorhot idag är känt mot kemiindustrin (september 2019) är den en potentiell måltavla. Avsiktliga skadliga handlingar kan spänna från enstaka stölder med begränsade konsekvenser, till terrorattentat och aktioner av stora aktörer som allvarligt kan påverka både den egna verksamheten och samhället i stort. Hoten kan komma från utomstående på plats eller utifrån, exempelvis via internet, men även från ”insiders”.

Mer om hotbild i **bilaga 2**

När ni dimensionerar ert skydd av verksamheten, är det bra om ni har en bild av vilka hot som kan finnas mot denna. Att göra detta utifrån NCT:s övergripande hotbild mot Sverige är en utmaning och för att underlätta ert arbete med detta finns en kortfattad generell hotbild avseende kemiska hot i bilaga 2. Frågor ni kan ställa er är vilka aktörer som kan ha intresse av era kemikalier, er infrastruktur och er information? Är ert företag aktivt i andra länder som kan ha en hotbild riktad mot sig? Finns det anledning för er att reagera om terrorhotnivån höjs? För säkerhetsskänslig verksamhet som omfattas av reglerna om säkerhetsskydd finns en särskild vägledning från Säkerhetspolisen.[4]

Även om någon detaljerad hotbild inte är möjlig att ta fram för just er verksamhet kan ni ändå arbeta med att förbättra skyddet i verksamheten på en grundläggande nivå.

3. Se vidare information om NCT hos Säkerhetspolisen, www.sakerhetspolisen.se/kontraterrorism.html.
4. Se vidare information om säkerhetsskydd hos Säkerhetspolisen, www.sakerhetspolisen.se/sakerhetsskydd.html.

5. Händelser och deras effekter

Effekterna av en terrorattack eller annan händelse med kemikalier kan vara allt från begränsade till katastrofala och kan påverka såväl verksamheten själv som omkringliggande verksamheter, människor, miljö och samhället. Utifrån de kemiska produkter och den infrastruktur ni identifierat, med invägande av hotbilden, fundera kring vilka händelser som skulle kunna inträffa och hur allvarliga konsekvenserna skulle kunna bli.

Kan en allvarlig händelse inträffa på er verksamhet eller med hjälp av kemiska produkter som kommer från er?

Exemplen nedan är inte uttömmande – tänk igenom ytterligare händelser som skulle kunna vara aktuella för just er verksamhet.

5.1 Utsläpp av kemikalier från verksamheten

Direkta utsläpp av större mängder kemikalier kan ge mycket stora konsekvenser. Det gäller särskilt utsläpp av giftiga gaser som sprider sig snabbt över ett stort område. En viktig parameter för konsekvenserna av denna typhändelse är närhet till bebyggelse där människor finns som kan exponeras för utsläppet. Utsläpp som innebär konsekvenser för trafiken på viktiga genomfartsleder kan också behöva vägas in.

Risken för utsläpp av kemikalier bör beaktas i ert normala olycksförebyggande arbete och särskilt om verksamheten berörs av den så kallade Sevesolagstiftningen[5]. Även vid en avsiktlig händelse kan mycket av det arbete som görs i olycksförebyggande sammanhang (riskanalyser, säkerhetsrapporter, handlingsprogram, m.m.) vara ett stöd vid bedömningen av effekter och konsekvenser av ett avsiktligt attentat.

5.2 Explosion eller brand i verksamheten

En explosion eller våldsam brand i verksamheten kan vara förödande rent materiellt och kan orsaka följdverkningar som t.ex. utsläpp av kemikalier. En större explosion eller brand kan också få allvarliga konsekvenser för omkringliggande bebyggelse och anläggningar, inklusive kritiska verksamheter som vatten- och elförsörjning samt IT-system. Dokumentation som tagits fram i olycksförebyggande syfte kan även här vara till nytta (se avsnitt 5.1).

5. Förordning (2015:236) om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor. Se även www.msb.se sök ”Seveso”.

5.3 Utsläpp av kemikalier på andra platser

Kemiska produkter som stulits eller köpts från verksamheten kan användas för att åstadkomma skada på andra platser. Det kan röra sig om giftiga kemikalier eller om utgångsämnen för tillverkning av giftiga kemikalier, t.ex. kemiska vapen.

5.4 Explosioner på andra platser

Kemiska produkter som har explosiva egenskaper kan användas för att åstadkomma en sprängverkan. Bland terrorister är det också vanligt att sprängämnen tillverkas från i sig ofarliga utgångsämnen, så kallade sprängämnesprekursorer. Flera attentat i Europa har visat att detta är ett reellt problem som måste tas på största allvar. Stölder och misstänkta köp av denna typ av produkter måste därför rapporteras till polisen.[6]

5.5 Belastning på samhällets resurser och produktflöden

En aspekt som behöver vägas in är den belastning som en större händelse kan få på samhällets resurser, t.ex. på samtal till SOS-alarm och på blåljusfunktioner (ambulans, räddningstjänst och polis). Effekter på flöden av för samhället viktiga produkter i distributionskedjor kan också vara nödvändiga att inkludera i analysen (exempelvis drivmedel och vattenreningskemikalier).

5.6 Fabricerade händelser (”fake news”)

Precis som vid en verklig händelse kan en fabricerad händelse påverka verksamheten och samhället. Att trovärdig information (filmer, ögonvittnesskildringar, m.m.) om en fabricerad händelse med kemikalier (olycka eller attentat) sprids via media och andra kanaler är ett realistiskt scenario[7]. En fabricerad händelse kan ha syftet att skapa allmän oro och misstro i samhället, samt att ifrågasätta både myndigheters och verksamhetens trovärdighet. Det kan även ge belastning på samhällets resurser precis som vid en verklig händelse (se avsnitt 5.5).

6. Enligt reglerna om sprängämnesprekursorer. Se www.msb.se/prekursorer.
7. I september 2014 skedde en omfattande rapportering i sociala medier om en explosion i en kemisk anläggning i Louisiana som visade sig aldrig ha inträffat.

6. Orsaker till att en händelse inträffar

Vad inom er verksamhet skulle kunna leda till en allvarlig händelse med kemikalier? Skulle någon kunna stjäla eller komma åt kemiska produkter eller känslig information utan att det märks? Kan vem som helst ta anställning på företaget och få tillgång till kemikalier? Var på anläggningen är det enkelt att orsaka ett sabotage? Identifiera de delar av verksamheten som skulle kunna vara särskilt sårbara för ett angrepp, inklusive IT-sårbarheter. Är det möjligt att tex. ändra flöden, orsaka utsläpp, eller stoppa (delar av) processen? Var skulle ett eventuellt sabotage få störst effekt?

Hur kan hanteringen av kemiska produkter i er verksamhet leda till att en allvarlig händelse inträffar?

Ställ egna frågor kring exemplen på orsaker nedan och andra orsaker som ni kommer på för att identifiera vad som skulle kunna ske inom er verksamhet.

6.1 Angrepp på förvaringsställen

Förvaringsställen för kemiska produkter (förråd, cisterner, m.m.) är uppenbara platser för angrepp, vilket även omfattar tillfällig förvaring på lastplatser och i fordon i väntan på transport. Det kan handla om en mekanisk påverkan (t.ex. att en ventil öppnas eller en rörledning kapas) så att giftiga kemikalier släpps ut och sprids, eller ett förråd med brandfarliga/explosiva kemikalier som antänds. Här är produktens farliga egenskaper och mängden avgörande.

6.2 Fysiska ingrepp i processer

Med fysiska ingrepp menas att någon antingen manuellt ändrar en inställning eller gör detta från processtyrningspanelen inne i verksamheten. Det kan vara en ventil som ändrar läge så att flöden dirigeras fel, pumpar som stoppas eller ändras så att tillförsel av kemikalier eller process/kylmedier uteblir eller ändras, bortfall av strömförsörjning eller drivmedel, etc.

6.3 IT-angrepp

Många processystem är numera uppkopplade mot internet (avsiktligt eller inte) och blir därför sårbara för angrepp från hackare som från en annan plats kan ta kontroll över dem. Information kan också stjälas för att underlätta ett senare angrepp. IT-angrepp kan även komma från insidan, exempelvis genom att någon inne i verksamheten gör inställningar så att skyddade IT-system kan nås externt, att skadlig programvara laddas ner eller att hårdvara ansluts så att systemet försätts i osäkert läge. Även system som inte är exponerade mot internet är sårbara – exempelvis kan skadlig kod spridas genom USB-minnen.

6.4 Stölder

Stöld av de berörda kemiska produkterna kan ske på själva anläggningen eller under transport till eller från denna, och det behöver inte nödvändigtvis handla om stora mängder. Syftet med stölden kan vara att använda produkterna i ett attentat eller för att tillverka andra ämnen för samma ändamål. Det kan också röra sig om stöld av information som är kopplad till produkterna eller företaget, för planering av ett framtida attentat.

6.5 Köp från obehöriga

Ett sätt att komma över kemiska produkter kan vara att köpa dem av er – direkt eller över internet. En potentiell terrorist eller brottsling kan förmodas vilja dölja sin identitet i samband med köpet, exempelvis genom att använda kontanter eller andra betalningsmetoder som inte är spårbara. En legitim köpare kommer däremot att låta registrera sig med organisationsnummer som kan kontrolleras hos t.ex. Skatteverket och betala med fakturor från konton som kan spåras. Nya kunder och oväntade ordrar, betalnings- eller leveranssätt är indikationer som kan ge anledning till extra kontroller och frågor.[8]

6.6 Transporter utanför det egna området

Transporter av kemiska produkter utanför det egna området omfattas av särskilda regelverk som även omfattar brottsförebyggande aspekter.[9] Transporter är en svag länk för både stölder och attacker, och transporterna utförs ofta inte av den egna verksamheten utan av en extern aktör. MSB har vägledningsmaterial som behandlar detta område och någon fördjupning kring transporter görs därför inte i denna vägledning.[10]

6.7 Hot mot och utpressning av nyckelpersonal

Personal som har kunskap om eller tillgång till kemiska produkter och relaterad utrustning kan utgöra en målgrupp för en extern angripare. Genom hot och utpressning skulle de kunna tvingas att hjälpa till med ett angrepp eller en stöld.

8. Indikatorer för misstänkta transaktioner finns i MSB:s informationsmaterial till handeln ”Du kan göra skillnad! Sälj kemiska produkter på ett ansvarsfullt sätt” www.msb.se sök på publikationsnummer ”MSB749”.
9. Information om reglerna för transport av farligt gods finns hos MSB, www.msb.se sök på ”farligt gods”
10. Se www.msb.se, sök på ”transportskydd”.

7. Förebyggande barriärer

Genom barriärer (motåtgärder) kan ett attentat, en stöld eller annan avsiktlig händelse med kemiska produkter förebyggas, precis som olyckor kan förebyggas. Nedan beskrivs några exempel på förebyggande barriärer som kan vara relevanta i er verksamhet. Kanske har ni redan genomfört dessa eller andra åtgärder, eller har förslag på åtgärder som inte nämns här.

Vad kan ni göra för att minska risken för att era kemiska produkter används till att åstadkomma en allvarlig händelse?

7.1 Fysiska barriärer

Staket, låsta grindar, inpasseringskontroll, kameraövervakning och larm är exempel på fysiska barriärer som förhindrar eller försvårar obehörigas tillträde till verksamheten som helhet eller till vissa områden inom verksamheten. Förvaringsplatser för kemiska produkter och processer där de används kan exempelvis skyddas mot tillträde genom fysiska barriärer.

7.2 Organisatoriska barriärer

Särskilda ID-kort för verksamheten som bärs synligt gör det enklare för medarbetare att upptäcka en utomstående och dessa kan även användas för tillträdet till delar av verksamheten där kemiska produkter hanteras eller där känslig information finns. Kontroll vid in- och utpassering till verksamhetens område och rutiner för mottagande och ledsagande av besökare är viktigt.

Vid beställning och leverans av kemikalier kan det vara aktuellt att kontrollera att mottagare, avsändare och distributör är legitima, och om det skett några förändringar i tidigare leveransrutiner bör dessa bekräftas av en säker källa innan de genomförs. Kontrollsystem och regelbunden inventering av berörda kemiska produkter och andra tillgångar gör att t.ex. en avvikande förbrukning eller försvunna kemikalier upptäcks snarast.

Möjligheten att ha kontroll över entreprenörer och personal som utför outsourcade (dvs. utkontrakterade) arbetsuppgifter är normalt inte lika god som den över egen personal. Även om er egen verksamhet har kontroll över sina anställda kan en person med ont uppsåt ta sig in i verksamheten via andra företag som arbetar på ert område. Under t.ex. ett processtopp är det vanligt att antalet entreprenörer på området ökar och verksamheten kan då bli mer sårbar än vanligt. Det kan t.ex. vara aktuellt att endast ge entreprenörer behörighet till vissa områden under vissa tider och att göra närmare undersökningar av säkerhetsrutinerna hos företagen ni anlitar.

Outsourcing av arbetsuppgifter ger med nödvändighet behov av att utbyta information mellan er verksamhet och andra företag, och ni kan behöva fundera på vilken typ av information som förmedlas och hur den lagras.

7.3 IT-säkerhet

Se även **avsnitt 3.2**

Dimensionera skyddet mot angrepp på IT-systemen utifrån er bedömning känsligheten i den information som hanteras (se avsnitt 3.2). Riskbegränsning kan ske genom att helt undvika risken, t.ex. genom att hantera informationen på annat sätt, eller genom att införa säkerhetsåtgärder.

Exempel på säkerhetsåtgärder som kan införas i en IT-miljö är:

- flerfaktorsautentisering (dvs. att identiteten hos en användare kontrolleras på flera av varandra oberoende sätt)
- att dela på nätverken för ”kontors-IT” och för ICS/SCADA
- att begränsa rättigheterna inom IT-systemen.

Lösenord på utrustning som har levererats bör genast bytas till unika och starka lösenord, programvara bör vara godkänd och makron (t.ex. i ordbehandlingsprogram), tjänster och protokoll som inte används bör inaktiveras. Samla loggar som kan bidra till att upptäcka, förstå och återställa IT-systemen efter ett angrepp.

MSB har publicerat flera vägledningar och annat material om informations- och IT-säkerhet som kan vara till hjälp[11] och tillhandahåller en grundläggande utbildning i IT-säkerhet för användare [12].

7.4 Securitykultur – en medveten personal

Ett framgångsrikt recept i skyddet mot olyckor är att uppmuntra personal att rapportera även mindre incidenter (för att förhindra att de någonsin leder till olyckor). Detta yttrar sig med tiden som en säkerhetskultur som genomsyrar verksamheten och är avgörande för att förbättra säkerheten. Motsvarande securitykultur kan byggas upp som ett skydd mot avsiktliga händelser och ett befintligt olycksrapporteringssystem kan utökas till att även omfatta securityhändelser. I mindre verksamheter kan det handla om en direktkontakt med t.ex. den som är ansvarig för arbetsmiljön.

Informera därför personal inom verksamheten om att det finns en problematik och att det är bra att vara uppmärksam på misstänkta

11. Se även två vägledningar på www.msb.se ”Vägledning för processorienterad informationskartläggning” sök på publikationsnummer ”MSB493” och ”Vägledning till ökad säkerhet i industriella styrsystem” sök på publikationsnummer ”MSB718”.
12. Datorstödd informationssäkerhetsutbildning för användare (DISA) finns i flera nivåer, se www.msb.se sök på ”DISA” eller på publikationsnummer ”MSB396”.

personer, beteenden och händelser som ger en känsla av att det är något som inte stämmer. Det kan vara en utomstående som befinner sig på området och inte ger sig tillkänna, en nyanställd som uppträder egendomligt eller någon som varit anställd i många år som börjat bete sig annorlunda på senare tid. Det kan också vara att något upplevs som ovanligt på området eller i lokalerna, t.ex. underlig parkering av fordon på området eller nära staket/ingångar till verksamheten. En security-kultur medför t.ex. att det upplevs som normalt att bära ID-brickan synligt, att ställa frågor till personer man inte känner igen och att rapportera avvikelser.

Detta ska inte innebära en generell misstänksamhet mot allt och alla utan behöver göras på ett nyanserat sätt – det handlar ofta om en magkänsla om att något inte står rätt till. Det är viktigt för personalens trygghet att det är tydligt hur securityhändelser ska rapporteras och vem som kan kontaktas i olika frågor relaterade till skyddet, också om de själva blir utsatta för påtryckningar. De som är ansvariga för att ta emot rapporteringar behöver ha rutiner för när incidenter bör rapporteras vidare till polisen.

7.5 Utbildning och övning av personal

Att utbilda och öva personal och nyckelpersoner regelbundet gör det enklare att hantera en händelse och att hitta sårbarheterna innan ett ”skarpt läge” inträffar. Detta höjer också kompetensen hos de inblandade, tydliggör ansvarsförhållanden, ökar medvetenheten och håller frågan levande. Det kan vara allt från att testa larmrutiner, , hantering av media och vad som ska göras om något händer utanför kontorstid, till att se hur lång tid det tar att samla de personer som ingår i en krisorganisation. Förslagsvis ingår denna typ av utbildning och övning i verksamhetens ordinarie säkerhetsarbete och övningar, men som ett eget möjligt scenario.

7.6 Intern och extern kommunikation vid händelser – kommunikationsplan

En terrorhändelse, oavsett storlek och effekt, skapar förmodligen stora rubriker och reaktioner i media och i andra kanaler (sociala medier m.m.). Är verksamheten förberedd med en realistisk och bra kommunikationsplan kan det förhindra onödig oro och belastning på samhället, samt motverka eventuell spridning av falsk information (se avsnitt 5.6).

Se även **avsnitt 5.6**

8. Exempel på metod för att förbättra skyddet

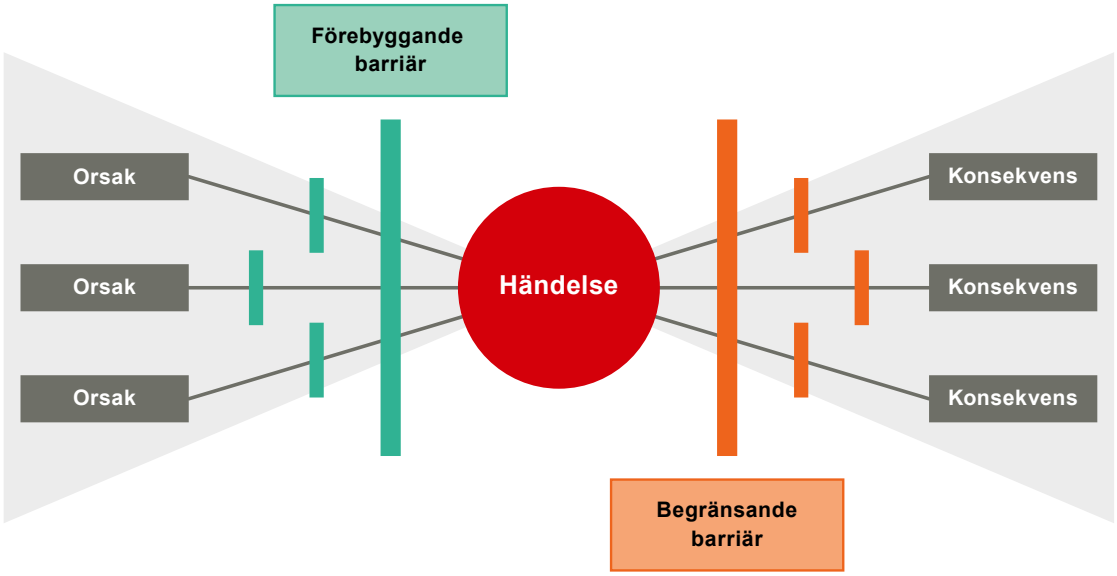
Bow tie-analys är en metod som kan användas för att förbättra skyddet.

Arbetet med att förbättra skyddet mot terrorism och annan brottlighet kan tyckas svårt och omfattande. Men det kan vara förhållandevis enkelt att åstadkomma ett förbättrat skydd – att täppa till de mest uppenbara hålen i den egna verksamhetens skydd behöver inte vara så besvärligt.

8.1 Bow tie-analyser

Ett förslag på en förhållandevis enkel metod att arbeta utifrån är en så kallade bow tie-analys (på svenska ibland kallad olycksfjäril). Metoden används vanligen i olyckssammanhang och ger en god överblick över alla orsaker, konsekvenser och motåtgärder (barriärer) på en gång i relation till en viss olycka. På vänstersidan i en bow tie beskrivs de förebyggande barriärer som ska förhindra att olyckan inträffar, och på högersidan beskrivs de begränsande barriärer som ska minska konsekvenserna av den om den ändå inträffar.[13]

Bow tie-analyser kan även användas i arbetet med skydd mot avsiktliga framkallade ”olyckor”. Med den terminologi som används i denna vägledning ser en generell bow tie ut som i figuren nedan.



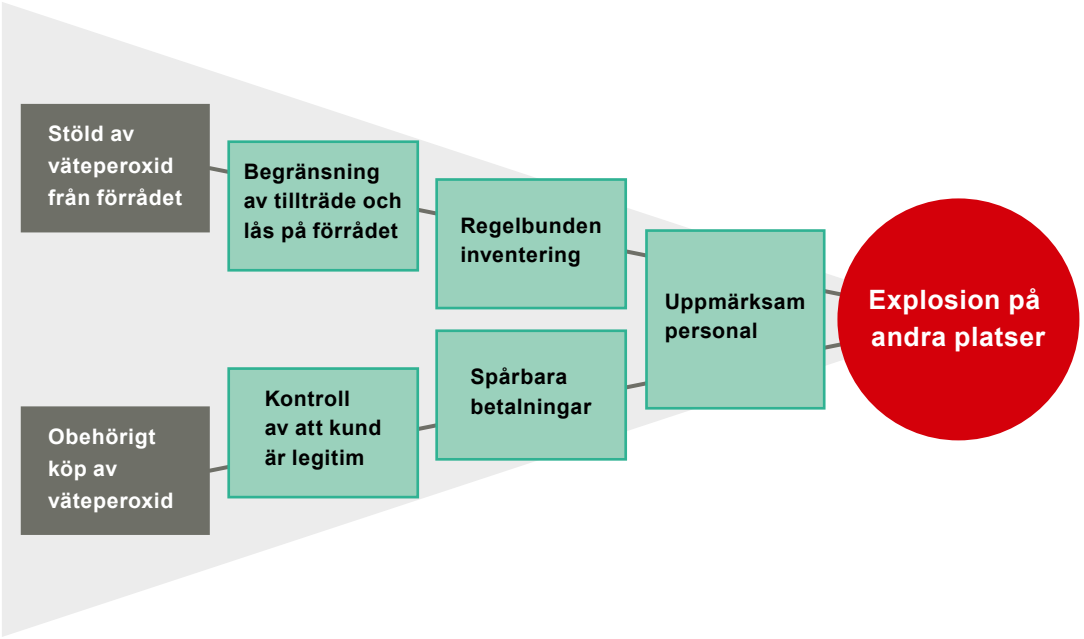
13. Beskrivning av metoden samt exempel på användning av bow tie-analys ur olycksförebyggande aspekt vid hantering av brandfarliga varor finns i MSB:s vägledning ”Riskanalys för mindre och medelstora verksamheter” www.msb.se sök på publikationsnummer ”MSB1060”.

Denna vägledning fokuserar på de förebyggande aspekterna, dvs. den vänstra delen av bow tien. Användandet av metoden i denna del skulle kunna göras på följande sätt:

1. Fundera på vilka händelser som skulle kunna inträffa, se t.ex. de olika händelserna och deras effekter i avsnitt 5. (Varje händelse behöver en egen bow tie.)
2. Fundera över vilka olika orsaker som skulle kunna leda fram till den aktuella händelsen, se t.ex. typorsakerna i avsnitt 6.
3. Fundera över vilka slags förebyggande barriärer som kan sättas in för att försvåra att en viss orsak faktiskt leder till händelsen i fråga, se t.ex. förslagen i avsnitt 7.

Se även **avsnitt 5, 6 och 7**

Figuren nedan visar ett exempel för att en explosion sker på andra platser (händelsen, se avsnitt 5.4) som följd av att väteperoxid (som kan användas för att tillverka sprängämnen) stjäls eller köps obehörigt från en verksamhet (orsakerna, se avsnitt 6.4 och 6.5) med några möjliga förebyggande barriärer (avsnitt 7).



Många av de begränsande barriärerna (den högra halvan av bow tien) bör redan finnas som resultat av ert olycksförebyggande arbete. Det kan dock vara värt att fundera på om det behövs ytterligare sådana barriärer kopplade till security, inklusive eventuell samverkan med polis, räddningstjänst och andra myndigheter samt kommunikation vid en händelse (se avsnitt 7.6).

8.2 Prioritera barriärerna och gör en handlingsplan

För att prioritera vilka förebyggande barriärer ni behöver fokusera på i första hand behöver ni väga in graden av allvarlighet i konsekvensen av en händelse. Var är det särskilt viktigt att sätta in barriärer?

Parametrar som kan behöva vägas in i den bedömningen är:

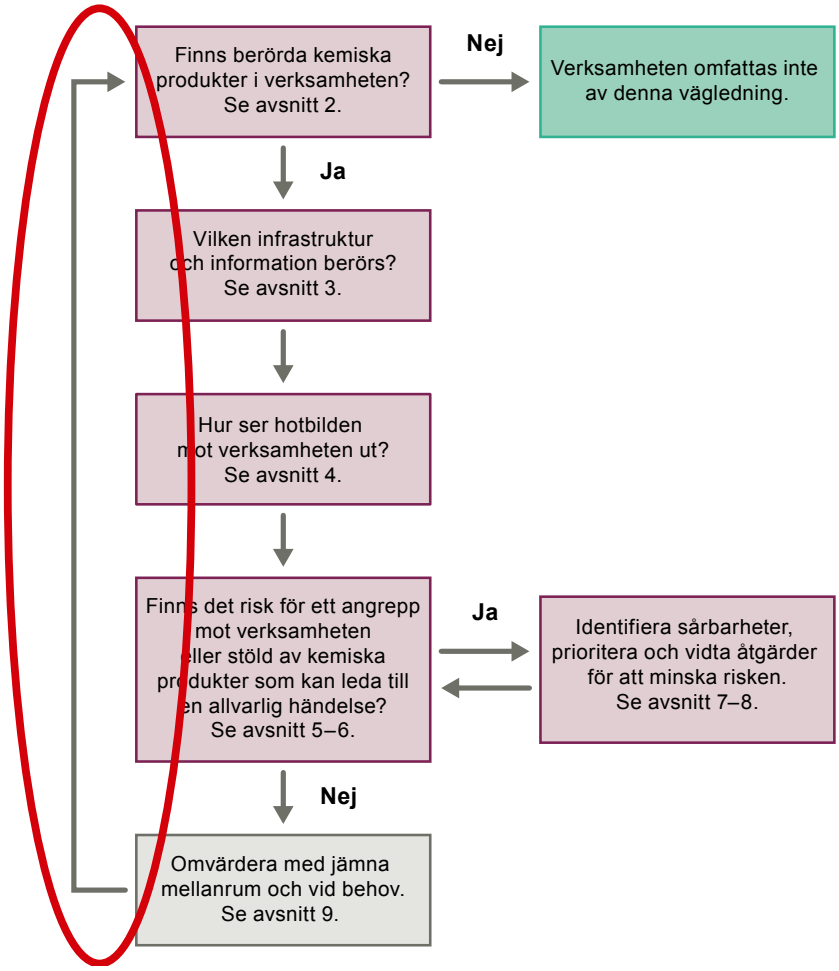
- skador på människor och antalet människor som kan beröras,
- materiella skador och skador på miljön,
- konsekvenser om stulna kemikalier används till kriminalitet/terrorism,
- värdet av förlorad information och vad den skulle kunna användas till,
- svårigheten att hantera händelsen, och
- utebliven funktionalitet för samhället (t.ex. kritiska leveranser).

Därefter behöver en handlingplan göras för att genomföra barriärerna i praktiken. En avvägning vad gäller barriärernas effektivitet (även i förhållande till kostnad) kan också behöva göras.

9. Omvärdera med jämna mellanrum och vid behov

Arbetet med skydd mot terrorism och annan allvarlig brottslighet är, liksom arbetet med skydd mot olyckshändelser, ett kontinuerligt förbättringsarbete som behöver följas upp löpande. Vid förändringar i verksamheten kan skyddet också behöva omvärderas, liksom vid en förändring av hotbilden eller vid höjd beredskap[14]. Händelser i andra delar av världen kan påverka företag med internationell verksamhet.

Skyddet mot terrorism och annan allvarlig brottslighet med kemiska produkter är ett löpande arbete.



14. Se vidare information på www.krisinformation.se, sök på ”höjd beredskap”.

Bilaga 1

Bilaga 1 – Berörda kemiska produkter

Kemiska produkter som har farliga egenskaper

I tabellen nedan listas farliga egenskaper hos kemiska produkter som mest uppenbart kan användas för att åstadkomma skada. För att enkelt kunna känna igen produkterna anges också hur de ska märkas vid överlåtelse (enligt CLP-förordningen[15]) och vid transport (enligt reglerna om transport av farligt gods[16]). Märkningen finns på förpackningar och information finns i avsnitt 2 (CLP) respektive 14 (transport) i produkternas säkerhetsdatablad.

Ämnesgrupp	Märkning
Akut giftiga ämnen	Märkta med symbolen ”dödskalle med korsade benknotor” samt faroangivelse som innehåller ordet ”dödligt” eller ”giftigt” (H300, H301, H310, H311, H330 eller H331 enligt CLP).
	  
Explosiva ämnen	Märkta med symbolen ”briserande bomben” samt faroangivelse som innehåller ordet ”explosivt” (H200, H201, H202 eller H203 enligt CLP).
	 
Oxiderande ämnen	Märkta med symbolen ”flamma-över-cirkel” samt faroangivelse som innehåller ordet ”oxiderande” (H271 eller H272 enligt CLP).
	 
Ämnen som utvecklar giftig gas i kontakt med vatten eller syra	Märkta med den kompletterande faroinformationen ”Utvecklar (mycket) giftig gas vid kontakt med vatten/syra” (EUH029, EUH031 eller EUH032 enligt CLP).

15. EU-förordning 1272/2008 om klassificering, märkning och förpackning av ämnen och blandningar. Kemikalieinspektionen är ansvarig myndighet för dessa i Sverige, se www.kemi.se/lagar-och-regler/clp---klassificering-och-markning.

16. Reglerna om transport av farligt gods betecknas ADR för transport på väg och RID för transport på järnväg. MSB är ansvarig myndighet för dessa regelverk i Sverige, se www.msb.se/sv/Forebyggande/Transport-av-farligt-gods/.

Utgångsämnen (prekursorer) till explosiva och mycket giftiga kemikalier

Vissa ämnen kan användas till att tillverka explosiva eller mycket giftiga kemikalier. Kemiska produkter som innehåller dessa ämnen behöver i sig själva inte ha farliga egenskaper och därför inte heller någon märkning för detta.

Om det aktuella ämnet är huvudkomponent i produkten anges detta normalt sett på förpackningen. Tänk på att även blandningar som innehåller berörda kemiska produkter bör tas med i genomgången om halten av aktuella ämnen är hög eller blandningen innehåller ett fåtal andra ämnen (så att aktuella ämnen skulle kunna utvinnas ur blandningen). Infomation om ingredienser ska finnas i säkerhetsdatabladets avsnitt 3.

- **Sprängämnesprekursorer**
  Följande ämnen listas i EU-förordning 98/2013 om saluföring och användning av sprängämnesprekursorer.[17]

Väteperoxid	Nitrometan	Salpetersyra
Kaliumklorat	Kaliumperklorat	Natriumklorat
Natriumperklorat	Hexamin	Svavelsyra
Ammoniumnitrat	Kalciumnitrat	Kalciumammoniumnitrat
Kaliumnitrat	Natriumnitrat	Magnesiumnitrat
Aceton	Aluminiumpulver	Magnesiumpulver

  För dessa ämnen gäller särskilda regler, bland annat krav på rapportering av misstänkta transaktioner och betydande stölder/försvinnanden till polisen. MSB har gett ut särskild vägledning om detta som kan vara aktuell att ta del av.[18]

- **Kemvapenprekursorer**
  Konventionen mot kemiska vapen (CWC) reglerar både kemiska vapen och utgångsämnen (prekursorer) för tillverkningen av sådana. De finns listade i kemikaliebilagan till konventionen. I Sverige är det Inspektionen för strategiska produkter (ISP[19]) som är nationell myndighet för kemvapenkonventionen.

  De ämnen som kan användas som kemiska vapen är alla i sig själva giftiga, vilket ligger i sakens natur. Även många av prekursorerna är i sig själva giftiga, och dessutom ganska exklusiva kemikalier

17. Se www.msb.se/prekursorer för mer information.
18. Se ”Du kan göra skillnad – sälj kemiska produkter på ett ansvarsfullt sätt” sök på publikationsnummer ”MSB749”.
19. Se www.isp.se/kemikalier/konventionen-mot-kemiska-vapen.

som inte förekommer annat än i högt specialiserade verksamheter. Några av dem är dock mer vanligt förekommande i kemiska produkter och verksamheter, exempelvis vissa fosfor- och fosforoxyklorider, alkylfosfiter, svavelklorider och tionylklorid, samt etanolaminer.

Övriga kemiska produkter

Se även **avsnitt 2.2**

Som beskrivet i avsnitt 2.2 i denna vägledning är det ett omfattande arbete att identifiera alla tänkbara kemiska produkter som kan användas för att åstadkomma skada och detta kräver expertkunskaper. Utöver produkternas egenskaper kan även sammanhanget vara relevant i en sådan bedömning. Exempelvis är många brandfarliga gaser och vätskor mycket lättillgängliga i samhället (så som gasol och bensin), varför det inte är rimligt att tro att dessa skulle behöva stjälas från en kemisk industri. De mängder som behövs för att vålla allvarlig skada kan också behöva vägas in.

Även om det generellt kan sägas att en kemisk produkt som klassificerats och därför märkts som farlig med avseende på olycksrisken också kan användas för att åstadkomma avsiktlig skada, behöver en bedömning göras av graden av fara och sammanhanget i övrigt. Detta är inte möjligt att göra på en övergripande nivå utan kräver kännedom om den specifika situationen.

I reglerna om transport av farligt gods på väg (ADR[20]) finns i kapitel 1.10 en lista över farligt gods med hög riskpotential där en avvägning har gjorts med avseende på farliga egenskaper hos en produkt och relevanta mängder vid transport. I den så kallade Seveso-förordningens[21] bilaga 1, del 1, finns motsvarande lista med avseende på konsekvenserna av storskaliga kemikalieolyckor i en stationär verksamhet. Även om dessa förteckningar kan vara användbara vid tillämpningen av denna vägledning behöver det hållas i minnet att dessa har sammanställts för andra ändamål.

20. MSB:s föreskrifter (MSBFS 2018:5) om transport av farligt gods på väg och i terräng (ADR-S).

21. Förordning (2015:236) om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor.

Bilaga 2

Bilaga 2 – Kortfattad hotbild

Det internationella hotet från kemiska attacker från såväl terrorism som aktörer med kopplingar till stater har fått ökad uppmärksamhet de senaste fem åren, på grund av att konstaterade attacker har genomförts och att andra har kunnat förhindras i förberedelsefasen (Interpol, Europol, FBI m.fl.).

I Sverige är terrorhotet förhöjt (januari 2018), vilket enligt Säkerhetspolisen innebär att ett terrordåd kan inträffa. Hotnivån är baserad på den bedömning som Nationellt centrum för terrorhotbedömning, NCT, gör varje år. Det säkerhetspolitiska läget i vår del av världen har blivit allt sämre. Exemplen på desinformation, vilseledning och påverkansoperationer blir allt fler. Att detta agerande även innefattar kemiska vapenaspekter, aktualiserat i Syrien och Storbritannien, går inte att bortse ifrån.

Största terrorhotet kommer för närvarande från våldsbejakande jihadism. Terrororganisationer som Daesh/ISIS och al-Qaida har anhängare inom den globala jihadistiska rörelsen, som även finns i Sverige. Dessa organisationer har avsikt och förmåga att förutom utföra terrordåd med hemgjorda bomber, knivar och fordon även sprida giftiga ämnen, vilket också skett i Irak och Syrien samt kunnat avvärjas i väst.

Ensamagerande anhängare eller små terrorceller i väst uppmanas att genomföra små och storskaliga terrorattentat. Aktuella uppmaningar och praktiska instruktioner hur detta ska göras inkluderar för närvarande även att tillverka, anskaffa och använda giftiga ämnen och sprängämnen och för detta använda kemikalier, material och anskaffningskällor som finns tillgängligt. Hotet kommer därmed från kemikalier och produkter med dubbel användning, PDA, eller dual-use chemical materials, farliga ämnen och utgångsämnen (prekursorer) som används av industrin, i det civila samhället och på laboratorier. Anhängare har kunnat få realtids-vägledning på distans genom viral kommunikation från individer med expertkunskap, som sannolikt befinner sig i konfliktområdet i Mellanöstern. Att säkra farliga ämnen, prekursorer, anläggningar, distributionskedjan och transporter, fysisk och digital information och nyckelpersoner mot denna typ av antagonistiska hot är därmed av största vikt att hantera i ert säkerhetsarbete. Även uttalade hot och falska påståenden behöver hanteras för att inte orsaka negativa effekter för verksamheten. Det gäller även risken att individer med tillträde påverkas eller har egen agenda att utföra antagonistiska handlingar, så kallade insiders. Samverkan, planering och dialog, inom er verksamhet och med brottsförebyggande myndigheter och andra inblandade för dessa frågor är viktigt för att skapa en god securitykultur och aktualitet för att bemöta detta antagonistiska hot.

Den kemiska industrisektorn i Sverige kan utgöra en måltavla och användas som verktyg för antagonister som har som syfte att skada individer, infrastruktur, en verksamhet eller Sveriges säkerhet. Att kemikalier och redskap kan förvärvas för att användas senare och på annan plats sätter en ytterligare dimension på risken för kemiska attacker, så även att kemi- och drivmedelsanläggningar kan ligga nära annan sårbar infrastruktur och skada denna om ett utsläpp, brand eller explosion skulle ske.

Några exempel på faktiska händelser som illustrerar bredden av aktuellt hot:

- I Frankrike skedde 2015 två terrorattentat, ett mot en petrokemisk verksamhet där två cisterner exploderade samt upptäckt av en spränganordning på en tredje. Det andra attentatet ägde rum mot en kemisk industri då en chaufför med behörighet till anläggningen körde in sitt fordon i en byggnad med gasflaskor med inerta gaser under tryck, för att få dem att detonera.
- I Belgien 2016 fanns misstankar om möjlig förberedelse till en terrorattack mot en kärnanläggning då polis hos en terrormisstänkt upptäckt att en nyckelperson vid anläggningen hade övervakats.
- Ett petrokemiskt företag med en anläggning i Saudiarabien utsattes 2017 för ett cyberattentat med en skadlig kod som konstruerats för att interagera med SIS (Safety Instrumented Safety) med avsikt att antingen stänga ner processer eller sättas i osäkert läge. Attentatet bedöms haft som trolig avsikt att sabotera och orsaka en explosion.
- I Australien 2017 och Tyskland 2018 lyckades två planerade terrorattentat avvärjas genom samverkan mellan internationella underrättelsetjänster och lokal polis. Det första gällde försök att tillverka en hemgjord kemisk bomb som skulle producera svavelväte från två utgångsämnen och den andra gällde tillverkning i en lägenhet av det mycket giftiga toxinet ricin och en hemgjord bomb med metallkulor. Individerna hade via telegramkanaler haft kontakt med ”expertterrorister” som instruerat dessa individer hur de skulle skaffa utgångsämnen, utrustning och därefter tillverka ämnena samt utspridningsanordningar.

Mer om antagonistiska hot mot den kemiska sektorn kan läsas i rapporten: Antagonistiska hot och kemiindustrin – aktuellt hotbild [FOI-R--4785--SE, 2019].

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1426 - september 2019 ISBN 978-91-7383-962-4