TERRORSIKRING

En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015)

Utgitt av Nasjonal sikkerhetsmyndighet, Politidirektoratet og Politiets sikkerhetstjeneste

NSM

POLITIET
POLITIDIREKTORATET

PST
POLITIETS SIKKERHETSTJENESTE

Forord

Arbeidet med å forebygge terrorhandlinger er en viktig oppgave. Terrorhandlingene 22. juli 2011 viste nødvendigheten av å kunne håndtere ekstreme situasjoner, også uten forvarsel. Vi har ingen garantier for at nye terrorhendelser ikke kan skje. Trusselbildet når det gjelder terrorisme er komplekst, og dette gjelder også spionasje, sabotasje og annen alvorlig kriminalitet. I tillegg har teknologi og metoder utviklet seg. Dette krever at man tenker nytt og har gode systemer for å kunne tilpasse sikringstiltakene, slik at de er relevante for det aktuelle trusselbildet.

Ved et terroranslag er virksomheten alene om å håndtere situasjonen inntil reaksjonsstyrker er på plass. Å ha gjort gode forberedelser både innen forebyggende sikkerhet og beredskap er et kollektivt samfunnsansvar, som enhver virksomhet bør kunne ivareta. De enkelte virksomheter har et ansvar for å sikre egen aktivitet, inkludert personell, informasjon og infrastruktur. Dette innebærer en forpliktelse til å planlegge egne sikringstiltak samt drifte og vedlikeholde disse.

Sikkerhets- og beredskapsarbeidet er et lederansvar, men berører alle nivåer i virksomheten. Det er viktig at arbeidet får den prioritet og den oppmerksomhet som kreves. Det bør legges vekt på at sikkerhetsarbeidet er forankret i ledelsen, og at tiltak er allment kjent og forstått.

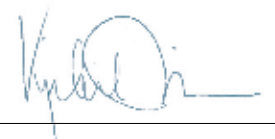
Veilederen er tiltenkt å være et hjelpemiddel for den enkelte virksomhet i å systematisere og tilpasse egne sikringstiltak i forhold til verdiene virksomheten ønsker å beskytte, aktuelle trusler og sårbarheter som kan utnyttes. Virksomhetene må gjennom egne tiltak kunne gjennomføre balanserte tiltak, som kan være både permanente og midlertidige, alt etter trusselsituasjonen.

Politidirektoratet (POD), Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM) håper at veilederen vil være et nyttig hjelpemiddel for sikkerhets- og beredskapsarbeidet internt i din virksomhet. Det viktigste er å forberede seg på det uventede: den største sårbarheten er *likegyldighet* overfor sikkerhet.

«Uten varsel – føre var»
Oslo, 30. september 2015

Marie Benedicte Bjørnland
Sjef
Politiets sikkerhetstjeneste

Odd Reidar Humlegaard
Politidirektør
Politidirektoratet



Kjetil Nilsen
Direktør
Nasjonal sikkerhetsmyndighet

Sikkerhetsråd

1. **Sikkerhet er et lederansvar.** Planlegg sikkerhet fra starten av ved alle typer endringer, prosjekter og programmer, slik som omorganisering, relokalisering eller lignende.

2. **Gjennomfør en sikringsrisikoanalyse av virksomheten** for å kartlegge hvilke verdier som må beskyttes, hvilke trusler virksomheten kan være utsatt for og hvilke sårbarheter som kan utnyttes. Forstå virksomheten opp mot de sikringsbehov som foreligger og beskytt verdiene med tilpassede tiltak.

3. **Virksomheten bør ha en hensiktsmessig organisering av sikkerhets- og beredskaps-arbeidet med en utpekt sikkerhetsleder og et styringssystem.** De ansatte skal være kjent med sikkerhetsinstrukser, sikkerhetsrutiner, evakueringsplaner, samt være årvåkne overfor aktuelle trusler.

4. **Sørg for grunnsikring i normalsituasjonen.** Dette er virksomhetens eget ansvar. Man kan ikke forvente forvarsel om terrorhandlinger. Fysisk sikring beskytter både informasjon, objekt og personell.

5. **Hold orden i bygg og publikumsområder, sørg for at de er godt opplyst.** Vurder å begrense adkomstspunkter og sørg for at ansatte, besøkende og kjøretøy har adgangs-tegn. Hvis det er mulig, unngå at kjøretøy parkeres i eller i nærheten av bygningen.

6. **Lag et beredskapssystem for virksomheten med forberedte tiltak, som kan iverksettes ved endringer i trusselbildet eller dersom det skjer en hendelse.** Forbered påbygningstiltak ved skjerpet trussel, slik som adgangskontroll for ansatte, besøkende, kjøretøy, samt post- og varemottak.

7. **Ingen plan er bedre enn selve gjennomføringen.** Sørg for å gjennomføre øvelser for å teste beredskapsplaner og sikringstiltak. Dette gjelder eksempelvis mottak av terrortrusler, søkerutiner og evakuering ved sikkerhetshendelser.

8. **Vurder hvordan virksomheten best kan beskytte sensitiv informasjon og hvilke informasjonssikkerhetstiltak som er nødvendige.** Husk at det er nær sammenheng mellom fysisk sikkerhet og IKT-sikkerhet. Sørg for at virksomhetens viktigste funksjoner kan gjenopprettes dersom IKT eller eiendom blir utilgjengelig.

9. **Søk råd og opplysninger hos politiet og andre myndigheter.** Etabler gode rutiner for kontakt mellom virksomheten og politi/nødetater.

Innhold

003 Forord
004 Sikkerhetsråd
006 Formål og bruk av veilederen

008 **1. Terminologi, ansvar og roller**
009 1.1 Hvorfor skal man sikre seg?
009 1.2 Terminologi
010 1.3 Hva er terrorisme?
010 1.4 Ansvar og roller

014 **2. Prosess for utarbeidelse av virksomhetens sikringstiltak**
015 2.1 Introduksjon
015 2.2 Igangsetting og koordinering
016 2.3 Sikringsrisikovurdering
019 2.4 Vurdering av strategi
020 2.5 Vurdering av tiltak

022 **3. Beredskapssystem**
023 3.1 Virksomhetenes beredskapsnivåer
023 3.2 Fastsettelse av lokalt beredskapsnivå
024 3.3 Skjematisk fremstilling av beredskapssystemet
025 3.4 Virksomhetens tiltaksliste basert på beredskapsnivå
025 3.5 Kvalitetssikring av beredskap
027 3.6 Eksempel på bruk av tiltak i de ulike beredskapstrinn

028 **4. Anbefalt videre lesning**

Vedlegg A: Eksempler på sikringstiltak – virksomhet
A1: Adgangskontroll for personell og besøkende
A2: Adgangskontroll for kjøretøy
A3: Post- og varemottak
A4: Fysiske omgivelser
A5: Personell
A6: Handling ved mottak av bombe- og terrortrussel
A7: Evakuering ved bombe- og terrortrussel
A8: Rutiner for søk og funn
A9: Informasjons- og kommunikasjonsteknologi (IKT)
A10: Krisekommunikasjon

Vedlegg B: Eksempler på sikringstiltak – individ
B1: Tiltak for egenbeskyttelse
B2: Handling ved væpnet angrep

Formål med og bruk av veilederen

Formålet med denne veilederen er å gi offentlige og private virksomheter et hjelpemiddel, slik at virksomheten kan planlegge og iverksette sikringstiltak mot terrorhandlinger. Den metodiske tilnærmingen i veilederen, som beskrives i kapittel 2, kan også benyttes for å sikre seg mot spionasje, sabotasje og annen alvorlig kriminalitet. Erfaring fra andre land viser at sikringstiltak mot terrorisme også kan ha en forbyggende effekt mot annen alvorlig kriminalitet.

Den enkelte virksomhet er underlagt ulike krav som krever metodisk tilnærming og regelmessig oppfølging. Kravene kan være pålagt av myndighetene eller av en kunde som krever at man opererer i samsvar med ulike standarder. Det finnes flere standarder, metoder og verktøy for håndtering og analyse av risiko. Denne veilederen baserer seg på metodikken i NS 5831 og NS 5832 (med hovedvekt på NS 5832). Veilederen retter seg primært mot virksomheter som ikke er omfattet av sikkerhetsloven eller nasjonalt beredskapssystem (NBS), herunder sivilt beredskapssystem (SBS). For virksomheter som er omfattet av sikkerhetsloven eller NBS, gjelder kravene om påbygningstiltak som følger av disse.

Metodikken i denne veilederen skal munne ut i ulike sikringstiltak, som samlet skal utgjøre den balanserte sikringen. I en helhetlig tilnærming til sikring må ting gjøres systematisk og i riktig rekkefølge. Dersom virksomhetens sikring ikke er tilfredsstillende, må grunnsikringen prioriteres først. Veilederen omfatter ikke selve krisehåndteringsdelen av terrorhandlinger.

Noen virksomheter er mer utsatt enn andre, avhengig av virksomhetens formål, driftsform og lokalisering. Det vil være stor variasjon når det gjelder ulike virksomheters behov for sikringstiltak. Disse tiltakene skal være valgt ut i fra egne analyser, slik at spesielle forhold og situasjoner er tatt hensyn til.

Veilederen beskriver generelle, kjente prosesser og eksempler på allmenne tiltak. Dokumentene som virksomhetene utarbeider på bakgrunn av denne veilederen, vil imidlertid kunne være mer sensitive og derfor ha et skjermingsbehov. Årsaken til dette er at dokumentene vil beskrive ulike tiltak virksomheten planlegger å implementere ved ulike hendelser og trusselsituasjoner. Tiltakene iverksettes for å redusere sårbarheter, og slike sårbarheter skal ikke være åpent tilgjengelig. For private virksomheter er det ingen offentligrettslige krav som forlanger at slik type informasjon skal være allment tilgjengelig. For virksomheter underlagt sikkerhetsloven, vil det være aktuelt å sikkerhetsgradere disse dokumentene.

Informasjon om sikringstiltak vil være interessant for noen som kanskje vurderer å gjennomføre et anslag. I tillegg kan det være vanskelig eller umulig å velge andre typer tiltak, dersom de opprinnelig planlagte tiltakene blir kjent av uvedkommende. Det er derfor viktig å informere og motivere de ansatte om dette ved blant annet øvelser og trening.

Veilederen er delt inn i fire kapitler, som kan leses kronologiske eller hver for seg alt etter behov for veiledning i den enkelte virksomhet. Det anbefales imidlertid å følge veilederen kronologisk gjennom samtlige kapitler for en grundig gjennomgang av aktuelle vurderinger og tiltak.

Under følger en kort beskrivelse av hovedkapitlene i veilederen:

Kapittel 1:
Bakgrunn og beskrivelse av ansvar og roller
Kapittelet tar for seg bakgrunnen for å lage en veileder for sikkerhets- og beredskapstiltak mot terrorhandlinger og enkelte grunnleggende begreper innenfor forebyggende sikkerhet og beredskap. Det beskriver ansvar og roller innen sikkerhet i virksomhetene og hos relevante myndigheter.

Kapittel 2:
Prosess for utarbeidelse av virksomhetens sikringstiltak
Her beskrives prosessen som anbefales lagt til grunn for utvikling og implementering av sikringstiltak mot terrorhandlinger. Kapittelet viser hvordan virksomheten må gjøre en vurdering av egne verdier, trusler, sårbarheter og samlet risiko, samt utforme egne og konkrete mål med sikringstiltakene. Kapittelet presenterer ulike strategier for håndtering av risiko, og hvordan virksomheten kan kvalitetssikre beredskapssystemet gjennom kontinuerlig oppfølging.

Kapittel 3:
Beredskapssystem
Kapittel 3 viser en skjematisk fremstilling av et nivåbasert beredskapssystem, og tar for seg prosessen med å velge ut konkrete tiltak til de ulike beredskapsnivåene. Kapittelet tar også for seg metode for fastsettelse av lokalt beredskapsnivå, og viser den dynamiske sammenhengen mellom verdi, trussel og sårbarhet.

Kapittel 4:
Anbefalt videre lesning
Denne litteraturlisten inneholder relevant litteratur benyttet i utarbeidelsen av veilederen og annen anbefalt videre lesning innen sikring mot uønskede tilsiktede handlinger.

Vedlegg A og B:
Vedlegg – eksempler på ulike påbygningstiltak
Dette kapittelet inneholder eksempler i vedleggs form på sikringstiltak mot terrorhandlinger. Tiltakslisten er på ingen måte uttømmende, men må tilpasses situasjonen og virksomheten. Tiltaksforslagene er gitt plass etter ønske fra en rekke virksomheter i forbindelse med råd og veiledning fra NSM, PST og politiet.

1

Terminologi, roller og ansvar

1.1 HVORFOR SKAL MAN SIKRE SEG?

Dersom virksomheten er sårbar, øker muligheten for at en tilsiktet uønsket handling vil kunne gjennomføres. Sikkerhet er en forutsetning for både ens egen og samfunnets funksjonalitet. Konsekvensen av manglende sikkerhet kan i mange tilfeller overstige kostnadene ved enkle sikringstiltak. Riktig utført sikring er samfunnsøkonomisk fornuftig og lønnsomt. Samtlige sikringstiltak må være balanserte, ikke være for inngripende eller overstige den verdien de skal beskytte.

Noen gode grunner til å sikre seg er (i tilfeldig rekkefølge):

- Lovpålagte sikringskrav
- Ivaretagelse av liv, helse og miljø
- Ivaretagelse av virksomhetens funksjon, ressurser og drift
- Beskyttelse av økonomiske verdier
- Omdømme

Det er ikke bare de ulike virksomhetenes egne hensyn som medfører et behov for å sikre seg. Offentlige forvaltningsorganer og samfunnskritiske funksjoner har også en samfunnsplikt til å sikre seg mot terrorhandlinger.

1.2 TERMINOLOGI

Virksomhetene bør ha klart for seg hva som er deres eget ansvar innen forebyggende sikkerhet og beredskap. I denne veilederen vises det primært til terminologi slik den er definert innen Norsk Standard (NS) 5830 og lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). Terminologien nevnt under er begreper som går igjen i veilederen. Der hvor begrepene kun er relevante for det aktuelle avsnittet, er de definert i teksten.

Sikkerhet: reell eller oppfattet tilstand som innebærer fravær av uønskede hendelser, frykt eller fare.

Uønsket hendelse: hendelse som kan utsette en verdi for uønsket påvirkning.

Tilsiktet uønsket handling: uønsket hendelse som forårsakes av en aktør som handler med hensikt.

Sikring: bruk av sikringstiltak ved håndtering av risiko forbundet med tilsiktede uønskede handlinger.

Grunnsikring: kombinasjonen av sikringstiltak som ivaretar virksomhetens sikringsbehov ved normaltilstand.

Sikkerhetstruende virksomhet: medvirkning til eller gjennomføring av spionasje, sabotasje eller terrorhandlinger.

Forebyggende sikkerhet: tiltak som skal hindre eller redusere effekten av den uønskede handlingen. Disse gjennomføres før en uønsket handling finner sted, ideelt for å unngå handlingen i utgangspunktet. Dette er både menneskelige, teknologiske og organisatoriske tiltak.

Beredskap: forberedt evne til på kort varsel å kunne øke sikkerhetsnivå, håndtere en uønsket hendelse eller tilstand, eller evne til å gjenopprette tilfredsstillende tilstand etter en uønsket hendelse. Beredskap forebygger ikke at en uønsket hendelse finner sted, men er en forberedelse til hendelseshåndtering.

Krisehåndtering: tiltak man gjennomfører for å håndtere en hendelse eller andre ekstraordinære tiltak for å gjenvinne kontroll.

Reaksjonsstyrke: en etablert respons for å avskjære, hindre eller avverge en sikkerhetstruende handling. Mandat, type og styrke vil avhenge av den verdien som skal beskyttes.

Trusselaktør: individ, gruppering eller organisasjon som har en kjent eller antatt intensjon om eller kapasitet til å true en annens sikkerhet.

Påbygningstiltak: sikringstiltak som iverksettes i tillegg til eksisterende grunnsikring. Påbygningstiltak iverksettes ved endring i trusselbildet og er ideelt sett tidsbegrenset.

1.3 HVA ER TERRORISME?

Det finnes ingen entydig og presis definisjon av begrepet terrorisme. I norsk lovgivning er terrorbegrepet behandlet på ulike steder. Sikkerhetsloven definerer terrorhandlinger som: «ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer eller eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål».

I Norge er terrorvirksomhet ansett som kriminelle handlinger og omfatter bl.a. å sette menneskers liv eller helse i fare, ødeleggelse av eller alvorlig skade på eiendom, å forstyrre prosesser eller systemer som opprettholder et demokratisk styre eller samfunnets økonomiske velferd og virkemåte.

1.4 ANSVAR OG ROLLER

1.4.1 Sikkerhetsarbeid i de enkelte virksomhetene

Den enkelte virksomhet har et ansvar for egne forebyggende sikkerhetstiltak. Sikkerhet er et lederansvar. Virksomhetens leder må forsikre seg om at virksomheten har en effektiv intern organisering av sikkerhets- og beredskapsarbeidet, samt at sikkerheten er en del av det daglige arbeidet som ivaretas av ledere og ansatte. Virksomhetens leder bør være oppdatert på risikobildet og hvilke tiltak som iverksettes for å redusere risikoen.

Virksomhetene anbefales å peke ut en egen sikkerhetsleder. For virksomheter underlagt sikkerhetsloven er dette et krav. Sikkerhetslederen bør kunne rapportere direkte til virksomhetens øverste ledelse. Sikkerhetslederens oppgaver vil variere, men bør blant annet inkludere følgende:

- Forvalte interne sikrings- og beredskapssystemer
- Benytte råd og veiledning fra sikkerhetsmyndigheter til å gjennomføre verdi-, trussel- og sårbarhetsvurderinger
- Styre sikringstiltakene slik at disse er tilpassede og effektive, og sørge for at påbygningstiltak lar seg implementere til rett tid ved skjerpet trussel
- Fremskaffe kunnskap om sikkerhetssituasjonen og rapportere til virksomhetens øverste ledelse
- Tilrettelegge for en god sikkerhetskultur i virksomheten
- Gjennomføre interne øvelser og trening for å kontrollere at virksomheten kan respondere hensiktsmessig på terrorrelaterte trusler og hendelser, samt opprette og vedlikeholde kontakt med politiet

1.4.2 Nasjonal sikkerhetsmyndighet (NSM)

NSM skal legge forholdene til rette for god sikring av informasjon og objekter av betydning for nasjonale sikkerhetsinteresser. NSM har det daglige forvaltningsansvaret av sikkerhetsloven med forskrifter.

NSM fører tilsyn med sikring av skjermingsverdige objekter, der ikke egne sektortilsyn gjør dette.

NSM har ansvar for å koordinere håndteringen av alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon. NSM skal forebygge og bistå i forbindelse med nettbaserte angrep mot kritisk infrastruktur i Norge. NSM holder oversikt over sikkerhetssituasjonen i samfunnskritisk infrastruktur innen informasjons- og kommunikasjonsteknologi (IKT), og har til en hver tid et oppdatert IKT-trussel- og sårbarhetsbilde.

NSM gir råd og veiledning innen forebyggende sikring vedrørende objekt-, informasjons- og personellsikkerhet til alle virksomheter underlagt sikkerhetsloven.

1.4.3 Politidirektoratet (POD)

POD har ansvaret for faglig ledelse, styring, oppfølging og utvikling av politidistriktene og politiets særorganer, med unntak av Politiets sikkerhetstjeneste (PST). Sikkerhetsspørsmål som ikke faller inn under PSTs ansvarsområde, ivaretas av POD. Direktoratet har et samordnings- og koordineringsansvar i forbindelse med kriser og alvorlige hendelser som utfordrer kapasitet og kompetanse i et eller flere politidistrikt.

1.4.4 Politiets sikkerhetstjeneste (PST)

PST har som hovedoppgave å forebygge og etterforske lovbrudd som kan true nasjonens sikkerhet og selvstendighet, og skal bidra til å sikre viktige samfunnsinteresser og gjennom sin virksomhet være et ledd i samfunnets samlede innsats for å fremme og befeste borgernes rettsikkerhet, trygghet og alminnelige velferd. PSTs oppgaver er hjemlet og beskrevet i politilovens § 17b og § 17c.

Tjenesten benytter ulike metoder og arbeidsmåter. Sentralt står innsamling av informasjon i tilknytning til personer og grupper som kan utgjøre en trussel mot rikets sikkerhet, utarbeidelse av analyser og trusselvurderinger, etterforskning og andre operative tiltak. PST utgir årlig en nasjonal trusselvurdering.

PST skal gi bistand og råd ved gjennomføring av sikkerhetstiltak i forsknings- og undervisningsinstitusjoner, statsadministrasjonen og offentlige og private virksomheter av betydning for viktige samfunnsinteresser.

1.4.5 Politidistriktene

Politiets oppgave er å forebygge og bekjempe kriminalitet og andre forstyrrelser av den alminnelige orden, samt beskytte person, eiendom og all lovlig virksomhet. Terrorisme er en form for alvorlig kriminalitet, og således en oppgave for politiet å forebygge og bekjempe.

Hvert politidistrikt har et selvstendig ansvar for polititjenesten i eget distrikt. Politiets oppgaver kan blant annet være følgende:

- Gi generelle råd om forebygging av kriminalitet og råd om tiltak for å forebygge terrorhandlinger i samarbeid med PST

- Gi råd til offentlige og private virksomheter ved utarbeidelse av beredskapsplaner
- Respondere på og håndtere trusler og hendelser
- Beskytte og sikre personer og objekter etter særskilt vurdering, og ved behov kan politiet også få bistand fra Forsvaret
- Etterforske trusler og hendelser

Politiet har døgnkontinuerlig beredskap for å forebygge, begrense eller håndtere uønskede eller ekstraordinære hendelser og kriser. Til denne beredskapen benyttes innsatspersonell i forskjellige kategorier.

Politidistriktene skal ha oversikt over kritisk infrastruktur/kritiske samfunnsfunksjoner og andre trusselutsatte objekter. Dette kan danne grunnlaget for utarbeidelse av et eventuelt beredskapsplanverk. Ved en forhøyet trussel kan det være aktuelt for politiet å sikre et objekt med sikringsstyrker.

Sikringsstyrker skal:

- Være et tillegg til objektets grunnsikrings- og beredskapstiltak
- Forsterke sikkerheten ved objektet
- Være av tidsbegrenset varighet

Forsvaret kan bistå politiet med vakthold og sikring av objekter og infrastruktur dersom forutsetningene for dette er til stede, i henhold til «Instruks om Forsvarets bistand til politiet» (25. juni 2012). Dersom flere eller større hendelser inntreffer samtidig, vil politiet måtte foreta prioriteringer. Virksomhetene må i slike tilfeller ha en etablert og fungerende grunnsikring, foreta egne vurderinger av trusselsituasjonen og vurdere å heve beredskapsnivået for å ivareta eget sikringsbehov.

112

■ Ved mistanke om eller funn av mistenkelige gjenstander eller trusler om terrorhandlinger må politiet varsles umiddelbart på telefon 112.

02800

■ For andre henvendelser nås politiet på telefon 02800

2

Prosess for utarbeidelse av virksomhetens sikringstiltak

2.1 INTRODUKSJON

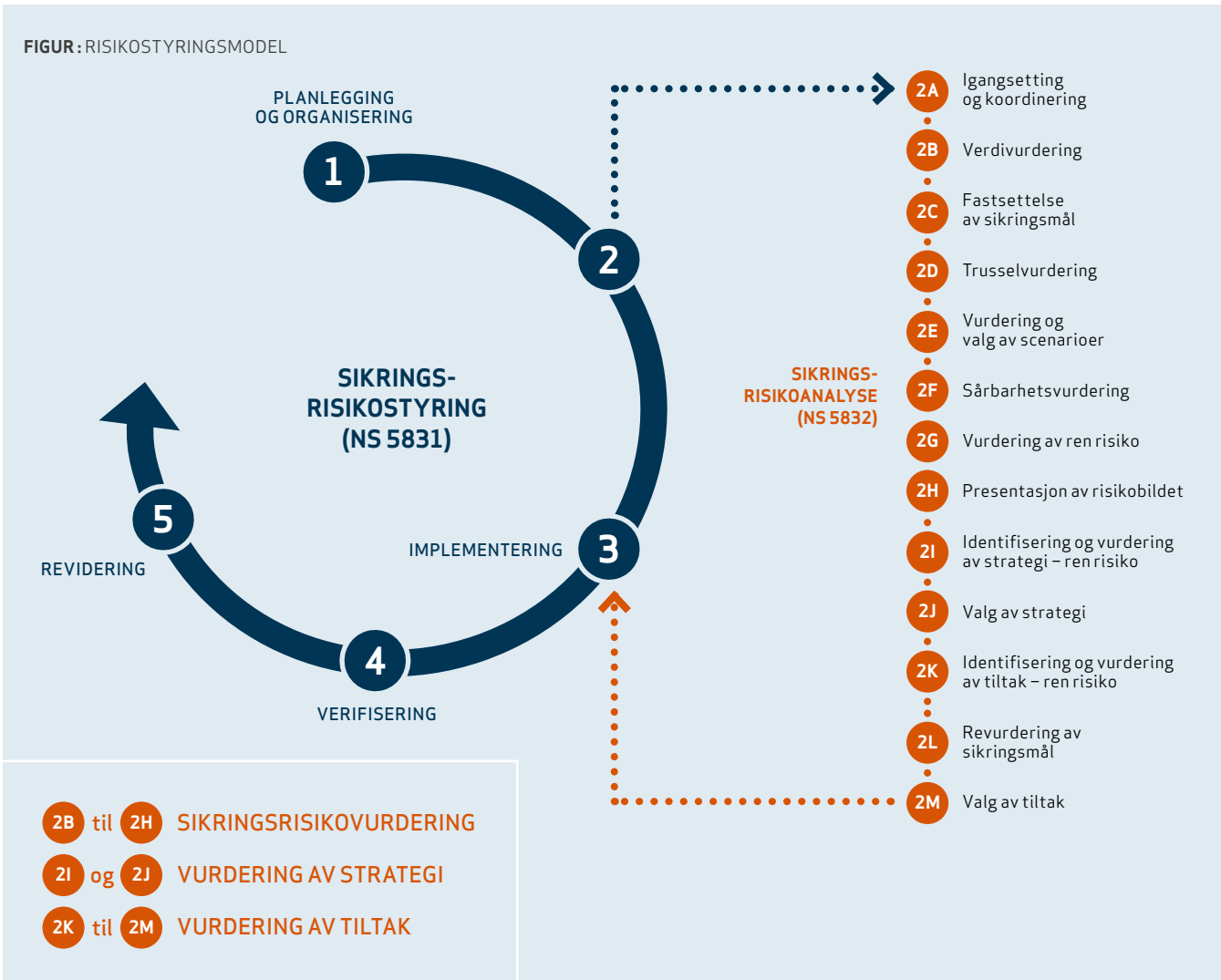
Dette kapittelet gjennomgår prosessen for utarbeidelse av virksomhetens sikringstiltak. Det er viktig at man har en strukturert tilnærming til dette arbeidet. Figuren under viser risikostyringsmodellen i henhold til NS 5831 og 5832. Denne illustrerer hvordan risikobasert sikkerhetsarbeid som prosess kan drives i virksomheten.

Veilederens fokus er på punkt 2 i sikringsrisikostyringen, selve sikringsrisikoanalysen, som beskriver en prosess som identifiserer nødvendige forebyggende tiltak og beredskapstiltak mot terrorhandlinger.

2.2 IGANGSETTING OG KOORDINERING 2A

Det er viktig at sikkerhetsarbeidet organiseres på en egnet måte og styres helhetlig av virksomhetens sikkerhetsleder. Dette er uavhengig av om det foretas en revisjon av eksisterende sikkerhetsorganisering og sikringstiltak, eller om virksom-

FIGUR: RISIKOSTYRINGSMODEL



heten skal etablere tiltak mot terrorhandlinger for første gang. Virksomhetens leder kan delegere myndighet, men er ansvarlig for ressurstildeling og forankring i organisasjonen. Sikkerhet betegnes som en tilstand, og ingen sikkerhetstilstand er uforanderlig. Det er hensiktsmessig å revidere sikringsstiltakene regelmessig.

Å informere og involvere alle berørte parter er viktig, fordi hele eller store deler av virksomheten blir påvirket av eventuelle sikringstiltak. Systemet som etableres er avhengig av de ansatte for å fungere som tiltenkt. Sørg for at alle som blir berørt av sikringstiltakene er informert og tilstrekkelig involvert.

Omfanget av prosessen avhenger av den enkelte virksomhets størrelse og verdier, samt krav til dokumentasjon. Der virksomheten mangler egen prosesskompetanse innen sikringsrisikoanalyse, kan det være nyttig å skaffe denne kompetansen eksternt. Det er likevel viktig at virksomheten involverer seg for å sikre kvaliteten. For å få et helhetlig og fullverdig produkt, må både kunnskap om virksomhetens funksjonalitet og sikringskompetanse samspille i en slik prosess. For en nærmere gjennomgang viser vi til NSMs veileder i sikkerhetsstyring.

2.3 SIKRINGSRISIKOVURDERING 2B til 2H

2.3.1 Verdivurdering

Det første trinnet i prosessen er en verdivurdering. Dette er en kartlegging og rangering av virksomhetens verdier.

Verdiene som man ønsker å beskytte kan være mange og ulike, for eksempel liv og helse, fysiske objekter og gjenstander og sikkerhetsgradert eller sensitiv informasjon. I tillegg har man mer abstrakte verdier som omdømme, operativ evne, bevegelsesfrihet med mer.

Eksempler på verdier som har beskyttelsesbehov:

- Personell
- Eiendom og anlegg
- Informasjon

Verdivurderingen bestemmer kvaliteten på den øvrige sikringsrisikoanalysen.

Få med dybden av virksomheten. Både intervjuer med ledelse og erfarne medarbeidere kan gi viktig informasjon. Still spørsmålet «hva om» ved ødeleggelse eller bortfall av ulike verdier.

Bruk tid på å kvalitetssikre verdivurderingen før man går videre i prosessen.

Eksempler på «hva om»

- Hva om vi ikke fikk kraftforsyning?
- Hva om våre IT- og telefonisystemer var nede?
- Hva om vi ikke fikk tilgang til nøkkelinformasjon?
- Hva om vi ikke kunne arbeide i virksomhetens lokaler?
- Hva om vi mistet personell gjennom et terroranslag?
- Hva om våre leverandører ikke kunne forsyne oss mer?
- Hva om vi ikke kunne betale våre leverandører eller våre kunder ikke kunne betale oss?

Ofte er det vanskelig å identifisere verdier som ikke kan omgjøres til en kroneverdi. Her kan det benyttes en skadevurdering i henhold til NS 5830, som er en vurdering av de negative konsekvensene for en eller flere verdier som følge av at en uønsket hendelse har inntruffet.

Ikke alle verdier er like verdifulle og like viktige å beskytte. Prioriteringen er vanskelig, men nødvendig for å unngå ressurskrevende og kostbare sikringstiltak.

Verdivurderingen legger premissene for det påfølgende arbeidet. Uten å ha avklart hvilke verdier man vil beskytte, vil man ikke kunne vite om sikringstiltakene har den ønskede virkningen. En god verdivurdering vil gjøre det øvrige sikringsarbeidet enklere, da man vil kunne definere og avgrense arbeidet til

den del av virksomheten der sikringsressursene bør prioriteres. Dette vil i sin tur kunne øke effekten av midlene som er tilgjengelig for iverksettelse av sikringstiltakene som blir besluttet gjennomført.

2.3.2 Fastsettelse av sikringsmål

Neste trinn er å bestemme hva virksomheten ønsker å oppnå med sikringstiltakene. Det skal fastsettes mål for hva som er ønsket eller akseptabel tilstand for verdiene under eller etter en uønsket hendelse. Hvilke mål virksomheten setter seg med sikringstiltakene, vil ha betydning for hvilke kostnader det medfører å beskytte seg.

Sikringsmålene kan revideres senere i prosessen, etter at man har vurdert ren risiko og valgt sikringsstrategi. Fastsettelse av sikringsmål er en forutsetning for å vurdere om tiltakene har den effekt de var tiltenkt. Sikringsmålene bør kunne utledes av virksomhetens overordnede mål.

Eksempler på sikringsmål:

- Virksomheten aksepterer ingen tap av eller påvirkning på identifiserte verdier tilhørende klassifisering X
- Grunnsikringen vår skal kunne beskytte oss mot trusselaktører av kategori X, mens påbygningstiltakene skal beskytte oss mot kategori Y
- Vi skal sørge for at den operative evnen ikke blir påvirket ved en eventuell hendelse, samt redusere skadene på øvrige verdier
- Fysisk inntrengning skal avverges i X antall minutter
- Det skal være mulig å evakuere trygt etter et fysisk anslag

2.3.3 Trusselvurdering

Trinn tre i prosessen er utarbeidelse av en trusselvurdering. Denne beskriver det gjeldende trusselbildet for det som ønskes beskyttet, og gir en vurdering av hvordan trusselbildet kan utvikle seg. Hovedfokuset er på reelle og potensielle trusselaktørers intensjon om og kapasitet til å ramme virksomheten. En slik vurdering kan ha mange hensikter. Den mest relevante er å identifisere trusselaktørenes kapasitet og handlingsmønster for å kunne utarbeide gode trusselscenarioer og dimensjonere sikringstiltakene riktig. I tillegg kan en trusselvurdering fungere som en tidlig varsling ved endringer i trusselbildet, slik at eksempelvis påbygningstiltak iverksettes.

I virksomhetens sikringsrisikoanalyse er det viktig at trusselvurderingen dekker et lengre tidsperspektiv. Trusselvurderingen bør også forsøke å identifisere hvilke faktorer som kan påvirke utviklingen negativt. Ved å følge med på disse faktorene, kan virksomheten identifisere fremtidige potensielle endringer i trusselbildet og iverksette forebyggende tiltak.

I utarbeidelsen av en trusselvurdering er det viktig å hente inn informasjon fra flere kilder. I tillegg til informasjon fra virksomhetens eller bransjens erfaringsdata, er det flere offentlige kilder som distribuerer relevant grunnlagsinformasjon for å utarbeide trusselvurderinger. Det gjelder blant annet PSTs årlige trusselvurdering, Etterretningstjenestens årlige vurdering og lokalt politi. I tillegg finnes det andre åpne kilder som kan bidra med relevant informasjon, for eksempel forskningsinstitusjoner og medier. For noen virksomheter vil PST utarbeide spesifikke trusselvurderinger hvis situasjonen tilsier det.

Relevante faktorer for en trusselvurdering kan være:

- Historikk – har egen eller lignende virksomhet vært truet tidligere?
- Tilstedeværelse – finnes det noen trusselaktører i området hvor virksomheten er etablert?
- Intensjon – har trusselaktøren et uttalt eller antatt ønske om å ramme virksomheten?
- Kapasitet – har trusselaktøren evne til å ramme virksomheten?

2.3.4 Vurdering og valg av scenarioer

Det fjerde trinnet er vurdering og valg av scenarioer. Det kreves kjennskap både til virksomheten og terrorisme for å finne relevante scenarioer. Med

et scenario mener vi her en tenkt situasjonsbeskrivelse, hvor en trusselaktør gjennomfører et terrorangrep. En utfordring ved valg av scenarioer er å kunne forutse trender innen terroraksjoner. Ved valg av scenarioer er det viktig at man forsøker å forutse nye metoder en trusselaktør kan benytte, og ikke bare ser på tidligere hendelser.

Det anbefales å ta utgangspunkt i kategorier av relevante angrepsmetoder for å finne aktuelle scenarioer (se tekstboks). Se gjerne på tidligere hendelser mot lignende virksomheter og ta høyde for utviklingstrekk i det fremtidige trusselbildet. Vurder disse opp mot neste steg: sårbarhetsvurderingen. Et godt scenario kjennetegnes ved at det er:

Eksempel på kategorier:

- Eksplosiver – på person eller kjøretøy, en eller flere bomber
- Bombetrussel – innringing eller hensatt gjenstand
- Væpnet angrep – en eller flere personer med stikk-, slag- eller skytevåpen
- Inntrengning med kjøretøy (rambukk)
- Gisselsituasjon – fysisk eller logisk (informasjonsnekt)
- Kjemisk/biologisk angrep

- Relevant – at det inneholder tilstrekkelig informasjon til å kunne være nyttig
- Konsistent – at noe som skjer et sted i scenarioet ikke utelukker noe som skjer et annet sted i scenarioet
- Plausibelt – at scenarioet er realiserbart, dvs. at det som scenarioet beskriver kan bli virkelighet

2.3.5 Sårbarhetsvurdering

Etter at det er foretatt valg av scenarioer må det foretas en sårbarhetsvurdering. En sårbarhetsvurdering er en vurdering av virksomhetens sårbarhet overfor identifiserte trusler mot identifiserte verdier. Sårbarhetsvurderingen beskriver i hvilken grad

Eksempel på scenarioer:

 # 1: En selvmordsbomber detonerer en medbrakt bombe i resepsjonsområdet. Det er på en av de travleste tidene i uken, hvor både ansatte er på vei til jobb og en større delegasjon besøkende venter i resepsjonsområdet.

 # 2: Arkivet/postmottaket åpner en pakke med anonym avsender, som inneholder en ukjent substans. Personene i umiddelbar nærhet blir uvel og viser symptomer på forgiftning. Postmottaket har felles ventilasjonsanlegg med resten av bygget. Det er fredag etter lunsj, og mange av de ansatte er på vei hjem.

eksisterende sikringstiltak, både grunnsikrings- og påbygningstiltak, vil kunne forhindre eller påvirke scenarioene som er beskrevet.

Et sentralt begrep i en slik vurdering er *mulighet*. I hvilken grad er det mulig for en trusselaktør å forsere virksomhetens sikkerhetstiltak? Graden av mulighet vil variere blant annet med hvilken kapasitet trusselaktøren har, eksempelvis hvilken kunnskap, ferdighet og verktøy trusselaktøren enten har eller kan tilegne seg.

Et hensiktsmessig hjelpemiddel for å vurdere effektiviteten av de eksisterende sikringstiltakene er «tidsregnskapet». Tidsregnskapet er tiden det tar fra angrepet oppdages og varsles, til angriperen kan påvirke verdien. Tiden angriperen bruker må være lengre enn tiden det tar før det reageres på en hensiktsmessig måte. Samlet skal sikringstiltakene kunne forsinke en trusselaktør nok til at man kan oppdage og avverge et angrep.

Det er viktig å forstå at enkelte tiltak kan gi en *opplevd* grad av sikkerhet uten å føre til *reell sikkerhet*. Man må derfor vurdere om helheten i sikringen faktisk møter de identifiserte trusselscenarioene.

2.3.6 Vurdering av ren risiko

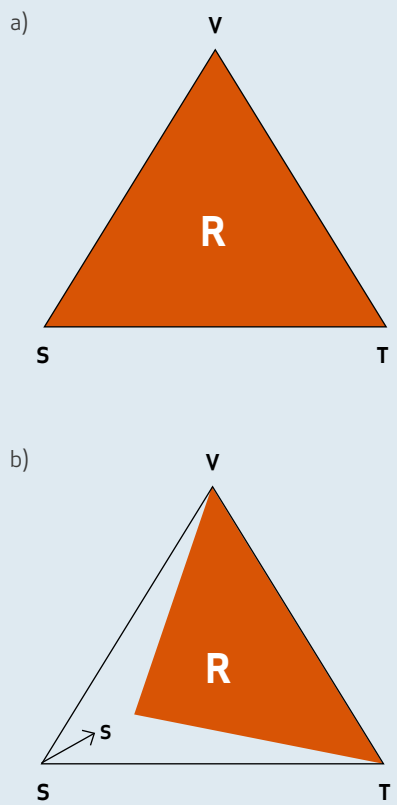
Etter sårbarhetsvurderingen må kunnskapen sammenstilles i en vurdering av ren risiko.

Denne vurderingen er ikke en kvantitativ men

en kvalitativ vurdering, blant annet fordi det kan være vanskelig å anslå trusselaktørenes intensjon og kapasitet. Den vil derfor alltid innebære en viss grad av subjektivitet og usikkerhet, men være forankret i kvaliteten på de forutgående vurderingene i sikringsrisikovurderingen (se prosessfigur i 2.1). Det kan være hensiktsmessig å beskrive usikkerheten i vurderingen.

Forholdet mellom verdi, trussel, sårbarhet og risiko illustreres i figur 1 under. Figur 1 a) viser en total risiko (R) som et utslag av forholdet mellom de tre variablene verdi (V), trussel (T) og sårbarhet (S). Arealet av trekanten illustrerer aktuell risiko for det valgte scenarioet. Figur 1 b) viser hvordan en reduksjon av en av variablene (i dette tilfellet sårbarhet), vil medføre en mindre total risiko. På samme måte vil en økning av en variabel også øke den totale risikoen.

FIGUR 1: RISIKOTREKANTEN



2.3.7 Presentasjon av sikringsrisikobildet

Trinn syv i prosessen er en presentasjon av det totale risikobildet. Her blir de ulike delvurderingene innen risiko sammenstilt slik at man får et godt overblikk. Hensikten er å kunne ta tak i de utfordringene som har blitt avdekket på en mest mulig effektiv måte. Sikringsrisikobildet presenteres beslutningstager for videre sikringsrisikostyring. Presentasjonen av sikringsrisikobildet vil derfor lede til en vurdering av strategier for håndtering av risiko.

2.4 VURDERING AV STRATEGI 2I og 2J

Neste trinn i prosessen er å undersøke hvilken strategi eller kombinasjon av strategier som det er mulig å benytte for å redusere eller fjerne den eventuelt uønskede risikoen som ble avdekket i sikringsrisikovurderingen.

Virksomheten har tradisjonelt fire ulike strategier å velge mellom. Disse er å unnvike risiko, overføre risikoen til andre, akseptere risiko eller å fjerne (redusere) risikoen.

2.4.1 Unnvike risiko

Når risikoen for tap eller skade er vurdert å være for høy, og det ikke er andre strategiske alternativer, må virksomheten vurdere om den skal la være å gjennomføre handlingen eller oppgaven.

Dette er ikke nødvendigvis en permanent beslutning, men kan være styrt av for eksempel en høy trussel i en kortere eller lengre periode. Dette kan kanskje være spesielt relevant for virksomheter som har begrensede muligheter til å forebygge en uønsket hendelse, og som i hovedsak må basere seg på en skadereduserende strategi.

Dette kan også være en mer permanent strategi, for eksempel om verdiene man forvalter eller eier er av en slik karakter at selv den minste risiko for tap eller skade er uakseptabel.

2.4.2 Overføre risiko

Overføring av risiko kan skje på flere måter. En variant er utkontraktering, hvor virksomheten betaler for at andre skal gjennomføre en handling eller oppgave. Eksempler på dette er utkontraktering av vakt- og sikringsoppgaver, verditransport og drift av IKT-systemer. Utkontraktering av oppgaver kan ha flere ulemper. Blant annet bør faktorer som de ansattes lojalitet, mulighet for kontroll ved ansettelser og kontroll av drift vurderes. Dette kan være spesielt viktig om tjenestene leveres og styres fra andre land enn Norge. Forsikring er et annet eksempel på overføring av risiko. Forsikring dekker økonomiske tap. I mange tilfeller er imidlertid verdiene ikke økonomisk mulig å forsikre, slik som markedsandeler og omdømme.

Vær oppmerksom på at overføring av risiko ikke fjerner selve risikoen. Det er fortsatt oppdragsgiveren som eier risikoen, selv om andre er engasjert til å utføre selve håndteringen.

2.4.3 Akseptere risiko

Aksept av risiko kan deles inn i to kategorier – *passiv* eller *aktiv*. Passiv aksept innebærer at virksomheten tar kostnaden for eller problemene med den uønskede hendelsen når den kommer ved å være såkalt selvassurandør. Aktiv aksept innebærer at virksomheten forventer et visst tap på bakgrunn av uønskede handlinger og setter av en sum penger eller har en akseptert tidsperiode for funksjonssvikt. Hva som er akseptabelt, vil variere etter virksomhet og situasjon. Den aksepterte risikoen man sitter igjen med etter å ha vurdert de ulike strategiene omtales som restrisiko.

2.4.4 Fjerne eller redusere risiko

Den risikoen som ikke kan overføres, unnvikes eller aksepteres må søkes redusert eller fjernet gjennom grunnsikrings- eller påbygningstiltak.

En måte å fjerne eller redusere risiko på, kan være gjennom *redundans*. Med redundans menes at virksomheten ved tap eller skade på en gitt verdi har mulighet til å erstatte funksjonen til denne verdien med en annen. Eksempler på dette er tilgang til strømaggregat ved bortfall av strøm.

2.5 VURDERING AV TILTAK 2K til 2M

Det siste trinnet i prosessen er vurdering av de tiltak som bør implementeres. For å oppnå målsetningen med å sikre verdiene, vil man ofte være avhengig av en kombinasjon av tiltak som virker sammen. Jo større og mer kompleks en virksomhet er, jo viktigere blir denne kombinasjonen. Tiltakene må tilpasses virksomheten. Det kan være hensiktsmessig å dele sikringstiltakene inn i tre kategorier, *menneskelige, teknologiske* og *organisatoriske*.

- Med *menneskelige* sikringstiltak menes tiltak rettet mot enkeltmennesker og grupper. Dette er psykologiske og sosiologiske tiltak, som påvirker adferd og reell evne til å bruke teknologiske sikringstiltak og følge organisatoriske sikringstiltak. Det kan også være tiltak som iverksettes av individer og/eller grupper for å hindre en uønsket hendelse, av mangel på teknologiske og organisatoriske tiltak. Denne kategorien er særlig viktig, da de to andre kategoriene raskt kan miste sin virkning om de menneskelige tiltakene svikter.
- Med *teknologiske* sikringstiltak menes fysiske, elektroniske og logiske sikringstiltak. I denne kategorien kan man finne ulike tiltak som kjøretøysperrer, automatisk innbruddsalarm, låssystemer, brannmur, virusbeskyttelse og lignende.
- Med *organisatoriske* sikringstiltak menes tiltak i form av skriftlige eller muntlige beskrivel-

Eksempel på viktigheten av menneskelige tiltak:

Konsulentselskapet AS kjøper inn dyre og sikre verdiskap til alle sine ansatte. De følger opp kjøpet med gode skriftlige instrukser om hvordan skapene skal låses og åpnes, og hvordan nøkler og koder skal oppbevares. De ansatte synes imidlertid løsningen er tungvinn, og de velger å oppbevare sine sensitive dokumenter i ulåste skuffer og skap. Effekten av de to første tiltakene blir fullstendig fraværende på grunn av mangelen på menneskelige tiltak gjennom bevisstgjøring av de ansatte.

ser, vurderinger og beslutninger som regulerer ledelse, organisering, prosesser, analyser, rutiner, atferd, eller anvendelse av andre sikringstiltak.

Når strategier og tiltak er vurdert og konsekvenser klarlagt, skal sikringsmålene revurderes. Det er virksomhetens leder som her skal vurdere akseptabel sikringsrisiko. På bakgrunn av dette besluttes sikringstiltak.

2.5.1 Synlige versus skjulte sikringstiltak

En annen avveining som må gjøres er hvilken synlighet og profil sikringstiltakene skal ha. Avgjørelsen av om man skal benytte skjulte eller synlige tiltak vil avhenge av situasjonen. Det er fordeler og ulemper ved begge alternativene. Fordelen med synlige tiltak er at de blant annet kan gi et signal om et sikkerhetspreg, som kan virke avskrekkende på noen trusselaktører. En ulempe kan være at synlige tiltak kan oppleves som skremmende og være lite attraktive for virksomheter med publikumskontakt.

Fordelen med skjulte tiltak kan være nettopp å unngå å skape unødig oppmerksomhet. En annen fordel kan være at en eventuell trusselaktør lettere kan bli identifisert, og kanskje forhindret, om de ikke kjenner til at tiltakene er blitt iverksatt, og for eksempel overvåkingen av et område har økt. Narretiltak kan også gjennomføres, slik at en øyensynlig sårbarhet fører angriper vekk fra den reelle verdien som skal beskyttes.

En kombinasjon av synlige og usynlige tiltak kan være nødvendig.

2.5.2 Sikkerhetsdesign og etterinstallering av sikringstiltak

Etterinstallering av sikringstiltak kan være meget kostbart. Det er viktig å kartlegge sikringsbehovene for en virksomhet, og disse behovene bør så tidlig som mulig vurderes i en byggeprosess eller omlokalisering.

Ved gjennomføringen av fysiske, elektroniske og logiske sikringstiltak, bør man forsikre seg om effektiviteten av tiltakene og at de harmoniserer med virksomhetenes øvrige tiltak og drift. Bruk eksperthjelp der dette er tilgjengelig, for å forhøre deg om beste praksis og eventuelle fallgruver ved de tiltakene som vil være aktuelle. Vær nøye ved vurderingen av hensiktsmessigheten og utformingen av kravspesifikasjonene for sikringstiltakene. Ha klart for deg hva som er grunnsikringstiltak og hva som er påbygningstiltak – og hvor lenge sistnevnte skal gjelde.

I tilfeller der det ikke er hensiktsmessig å benytte fysiske sikringstiltak, kan man bruke andre strategier for å redusere sårbarheten. Eksempler på dette kan være økt bruk av organisatoriske og aktive tiltak som årvåkenhet, overvåkning samt ulike skadereduserende tiltak.

3

Beredskapssystem

Et beredskapssystem er virksomhetens systematiske og kontinuerlige prosesser som planlegger, opererer, evaluerer og forbedrer det helhetlige arbeidet med beredskap. Hensikten med beredskapssystemet er at virksomheten på kort varsel kan heve sitt sikkerhetsnivå, håndtere en uønsket hendelse eller tilstand og gjenopprette tilfredsstillende tilstand etter en uønsket hendelse eller tilstand.

En beredskapsplan er de samlede dokumenterte instrukser og prosedyrer som konkretiserer virksomhetens handlinger ved en uønsket hendelse eller tilstand. Således kan beredskapsplanverket sees på som et element av det helhetlige beredskapssystemet.

En god grunnsikring og ansattes årvåkenhet kan hindre og begrense gjennomføringen av enkelte angrep. Påbygningstiltak vil ha liten eller ingen effekt ved anslag uten forvarsel. Et etablert beredskapssystem kan få virksomheten raskere tilbake til en normalsituasjon.

3.1 VIRKSOMHETENES BEREDSKAPSNIVÅER

Et beredskapssystem må være dynamisk og kunne følge endringer i virksomhetens risikobilde. Grunnsikringen kan omfatte adgangskontroll, låser, dører, alarmer, kameraovervåkning, belysning, gjerder, porter og fasader med mer. Beredskapsnivåene iverksettes i en tidsbegrenset og ekstraordinær situasjon. Virksomhetene bør tilpasse sine konkrete tiltak til disse beredskapsnivåene. Nedenfor beskrives fire nivåer i tillegg til grunnsikringen.

- **Første beredskapsnivå**
  Dette beredskapsnivået gir uttrykk for en endring eller usikkerhet i trusselbildet, hvis art og omfang er ukjent. Omstendighetene innebærer at det er behov for å styrke grunnsikringen og årvåkenheten på grunnlag av en potensiell trussel hvor det foreligger en mulig intensjon om eller kapasitet til å true virksomhetens sikkerhet.

- **Andre beredskapsnivå**
  Dette nivået benyttes når trusselbildet er skjerpet. Det innebærer en betydelig økning av sikringsnivået ved virksomheten, men den daglige driften skal fortsatt ivaretas.

- **Tredje beredskapsnivå**
  Dette nivået brukes når en virksomhet er utsatt for en reell trussel, hvor det er en kjent intensjon om og kapasitet til å true en virksomhets sikkerhet. Et slikt nivå medfører at drift og aktivitetsnivå ved virksomheten reduseres og vanskelig kan opprettholdes i mer enn korte perioder av gangen.

- **Fjerde beredskapsnivå**
  Dette beredskapsnivået innføres når en terrorhandling inntreffer, eller et terrorangrep mot virksomheten er umiddelbart overhengende. Virksomheten evakueres, reduseres betydelig eller alternativ funksjon overtar.

Det anbefales at beredskapsnivåene gis en betegnelse som er lett forståelig for den enkelte ansatte. Eksemplene nedenfor er i bruk i ulike virksomheter:

- Bruk av tall – beredskapsnivå I, II, III, IV
- Bruk av bokstaver – A, B, C, D
- Bruk av farger – (grønn, gul oransje og rød).
- Bruk av bokstaver i kombinasjon med farge – benyttes i NATOs beredskapssystem og NBS (A og B på gul bunn, C og D på rød bunn)

3.2 FASTSETTELSE AV LOKALT BEREDSKAPSNIVÅ

Beredskapsnivået bør i utgangspunktet fastsettes etter en risikoanalyse foretatt av virksomheten selv. Trusselen mot en virksomhet kan både være større og mindre enn det generelle trusselbildet. Dette krever en vurdering av den enkelte virksomhet, enten på bakgrunn av en hendelse eller en situasjon som krever ekstra tiltak. Endringer i virksomhetens *verdi* eller *sårbarhet* kan også påvirke risikobildet, og dermed hvilket beredskapsnivå virksomheten bør ha.

De beredskapsnivåer og tiltak som beskrives i denne veilederen er påbygningstiltak. Ikke alle beredskapstiltak er ment å skulle opprettholdes over lang tid. Dersom tiltakene må opprettholdes over lang tid, bør man vurdere å implementere dem i grunnsikringen. Tiltak som iverksettes kan være ressurskrevende og påvirke både ansatte og organisasjonen. Normaltilstand bør derfor gjenopprettes så snart dette er mulig og forsvarlig.

Eksempler på fastsettelse av beredskapsnivå

Eksempel A: Hendelsesstyrt heving av beredskap

Immigrasjonsmyndighetene i et naboland utsettes for et terrorangrep. Grupperingen som påtar seg ansvaret har sympatisører her i landet, men man kjenner ikke til deres kapasitet til å gjennomføre terrorhandlinger. Den offentlige institusjonen *Innvandringsverket* hever beredskapsnivået til andre beredskapsnivå inntil situasjonen er avklart.

Eksempel B: Potensiell trussel

Hovedkontoret til bedriften *Kullgass AS* blir underrettet om en troverdig trussel fra en terrorgruppe som motsetter seg deres virksomhet i utlandet. Mistenkte medlemmer av terrorgruppen er her i landet. Kullgass AS bestemmer seg for å iverksette tredje beredskapsnivå inntil situasjonen er avklart. Dette innebærer iverksetting av desentralisert funksjon med utstrakt bruk av hjemmekontor for de ansatte.

Eksempel C: Reell trussel

En bombetrussel ringes inn til *Offentlighetsdirektoratet*. Etter et gjennomført søk ved kontorene til direktoratet, blir det funnet en bombelignende gjenstand. Offentlighetsdirektoratet innfører fjerde beredskapsnivå på bakgrunn av funnet. De ansatte evakueres og direktoratets lokaler avsperres inntil assistanse fra nødetater ankommer og situasjonen håndteres videre.

3.3 SKJEMATISK FREMSTILLING AV BEREDSKAPSSYSTEMET

Figuren nedenfor viser hvordan et beredskapssystem kan bygges opp. Dette er et eksempel på oppbygning av beredskapsnivåer med tilhørende tiltak, som er en del av beredskapssystemet. Tiltakene er inndelt i menneskelige, teknologiske og organisatoriske kategorier, men for enkelhets skyld er det ikke skilt mellom forebyggende og skadereduserende tiltak.

Det er viktig at tiltakene i virksomhetens grunnsikring og tiltakene i beredskapssystemet består av en effektiv og hensiktsmessig kombinasjon som utfyller hverandre. Teknologiske grunnsikringstiltak ligger for eksempel ofte til grunn for organisatoriske beredskapstiltak.

	TILTAK		
BEREDSKAPSNIVÅ	Menneskelige	Teknologiske	Organisatoriske
Grunnsikring			
Første			
Andre			
Tredje			
Fjerde			

Eksempel på menneskelige, teknologiske og organisatoriske tiltak:

Acme AS har investert i sikre dører med et avansert elektronisk låssystem til alle sine adgangspunkter (et teknologisk forebyggende tiltak). I en normalsituasjon (grunnsikring) åpnes disse ved at ansatte holder adgangskortene sine foran kortleseren.

Ved beredskapsnivå 1 innføres også PIN-kode for å åpne dørene, og ved nivå 2 endres adgangen for de ansatte til kun å gjelde deres egne kontorer og andre tjenestemessige nødvendige deler av virksomhetens lokaler (organisatoriske forebyggende tiltak).

Ved første heving av beredskapsnivået innkalles alle ansatte til en orientering, der de blir informert om situasjonen som foreligger, og der viktigheten av å følge prosedyrer og være årvåken i forbindelse med adgangskontroll understrekes (menneskelige forebyggende tiltak).

3.4 VIRKSOMHETENS TILTAKSLISTE BASERT PÅ BEREDSKAPSNIVÅ

Virksomheten bør lage en tiltaksliste basert på eget risikobilde og eksisterende grunnsikring.

Tiltakslisten kan utformes på tre måter:

a) En fast liste med tiltak for hvert av de fire beredskapsnivåene, som innføres automatisk og uavhengig av årsaken til endringen i risikobildet
b) En liste med tiltak for hvert av de fire beredskapsnivåene, der tiltakene som skal iverksettes blir gjenstand for en vurdering på bakgrunn av den aktuelle situasjonen
c) En kombinasjon av a) og b)

De to sistnevnte modellene tar større hensyn til den spesifikke risikoen som foreligger. Virksomheten har da i større grad mulighet for å styre konsekvensene for den daglige driften ved kun å innføre de tiltak som synes hensiktsmessige. Disse modellene har større fleksibilitet. For eksempel vil det være mulig å benytte tiltak fra et høyt nivå på et lavere nivå og motsatt, men dette forutsetter kompetent sikkerhetsstyring.

De ansatte i virksomheten bør være kjent med hvilket beredskapsnivå som er gjeldende, og hvilke sikkerhetsrutiner som følger av dette. Det er derfor viktig med god internkommunikasjon, og at alle som har behov for det har tilgang til beredskapsplanene. Beredskapssystemet kan også brukes til å indikere behovet for å øke årvåkenheten, for eksempel ved at beredskapsnivået høynes men få eller ingen tiltak innføres.

Tiltakene kan systematiseres på en måte som gjør det enkelt å formidle hvilke tiltak som innføres ved en heving av beredskapsnivået, for eksempel 1a, 1b,... 2a, 2b, osv. der tallene representerer beredskapsnivået og bokstavene de ulike tiltakene.

3.5 KVALITETSSIKRING AV BEREDSKAPEN

Sikrings- og beredskapssystemer bør øves, testes, kontrolleres, vedlikeholdes og revideres regelmessig for å sikre at de fungerer som tiltenkt og er tilpasset virksomhetens behov. Eksterne så vel som interne faktorer kan og vil forandre seg, og planene må gjenspeile dette.

Det finnes flere måter å kvalitetssikre en virksomhets beredskapssystem på, og de vanligste beskrives her.

3.5.1 Øvelser

Øvelser er et tiltak for læring og kontinuerlig forbedring. Man bør derfor ikke være redd for å gjøre feil på en øvelse.

En øvelse bør ha en overordnet målsetting og en beskrivelse av hva man forventer å få ut av øvelsen. Øvelser kan være altomfattende og involvere alle aspekter av planverket og alt personell. De kan også være rettet mot et begrenset område, begrensede personellgrupper eller bestemte typer utstyr. Eksempel på en slik begrenset øvelse kan være å gjennomføre evakuering fra en bygning. Husk at man bør ha ulike evakueringsrutiner for ulike hendelser. En evakueringsplass kan også være et terrormål. Hyppigheten av øvelser vil være avhengig av blant annet virksomhetens struktur, risikobilde eller resultatet av tidligere øvelser.

Øvelsene bør teste om personell med særskilt ansvar kjenner til hvilke tiltak de skal treffe og hva som er deres rolle i det aktuelle scenariet, og om planlagte tiltak er godt kjent og innøvd. Øvelsene gir også en pekepinn på om ansatte er godt kjent med hvilke tiltak som treffes dersom en hendelse skulle inntreffe. Eksempler her er evakueringsplaner, tiltak for å sikre områder ved bombealarm, samlingsplasser osv.

I tillegg til å øve prosedyrer og tiltak, bør øvelsene omfatte testing og kontroll av nødvendig utstyr, for eksempel varslingsanlegg og kommunikasjonssystemer. Rutiner og ansvar for å kontakte nødetater og eventuell rapportering er også relevant å teste.

Like viktig som øvelsen selv er evalueringen etterpå. Evalueringen bør være en systematisk gjennomgang av øvelsen i ettertid for å identifisere forbedringspunkter. Dersom øvelsene avslører svakheter i planverk, prosedyrer og tiltak, må disse justeres. Det er viktig å ta vare på erfaringene. En øvelse skal kunne avdekke svakheter i beredskapshåndteringen. Det er her det gis mulighet til å rette feil før de skjer i virkelige hendelser.

Øvelser kan ha forskjellig form og være beregnet på forskjellige nivåer i virksomheten. Det er nødvendig å ha klart for seg hvilke nivåer som skal øves, slik at relevante problemstillinger blir spilt inn til de rette nivåene. De vanligste typer øvelser er:

- **Bordøvelser (tabletop):** En øvelsesform hvor tiltak ikke iverksettes reelt. Deltakerne samles rundt et bord. Problemstillinger blir spilt inn, og de enkelte deltagere legger frem sine bidrag til løsning. Hver problemstilling blir behandlet helt ut før neste blir lagt frem. En bordøvelse er ressursbesparende og kan gi deltagerne mer tid til rådighet enn i andre øvelsestyper, noe som gjør at deltagerne kan reflektere grundig rundt beslutninger.

- **Spilløvelser:** En egen spillstab styrer øvelsens gang. Øvingsdeltakerne jobber ut fra de posisjonene de ville hatt i et reelt tilfelle. Spillstaben gir innspill i tilnærmet sanntid etter en planlagt hendelsesoversikt (dreiebok). Øvelsen begrenser seg til at beslutninger blir tatt og tiltak blir beordret, men tiltakene blir ikke iverksatt. Avgjørelser må tas mens et scenario utspiller seg på samme måte som det ville gjort i en virkelig situasjon. Slike øvelser gir en høy grad av realisme uten å involvere store ressurser, samtidig som beslutningstagere får samarbeide slik de vil måtte gjøre i en reell situasjon.

- **Fullskalaøvelser:** En fullskalaøvelse er en praktisk innsatsøvelse. Øvelsen styres av en spillstab på lik linje med en spilløvelse, men i tillegg blir tiltakene, eller enkelte av tiltakene, satt ut i livet. Dette er en ressurs- og personellkrevende måte å øve på, men vil på en god måte få verifisert at tiltak fungerer hensiktsmessig og at personellet kjenner sine roller og innholdet i beredskapsplanen. En slik øvelse kan også være lærerik når det gjelder å koordinere innsats med eksterne aktører, eksempelvis politi og andre nødetater.

3.5.2 Kontroll og testing

Regelmessige kontrollrutiner er viktig for å sikre at nødvendig utstyr og rutiner fungerer som de skal. Eksempler på hva som bør være gjenstand for regelmessig kontroll er kontakt- og varslingslister, sperremateriell, back-up, strømforsyninger, informasjonsmedier, sambandsutstyr/kommunikasjonsmidler, førstehjelpsutstyr og brannslokkingsutstyr.

I tillegg kan det være hensiktsmessig å foreta regelmessige uvarslede tester av enkelte deler av beredskapssystemet. Slike tester vil bedre enn noe annet vise «tingenes reelle tilstand». Eksempler på dette er å gjennomføre en uvarslet evakueringsøvelse, eller å kontakte personell uten forvarsel og be dem iverksette prosedyrer og tiltak for et bestemt beredskapsnivå eller bestemte beredskapstiltak.

3.5.3 Vedlikehold og revidering

Beredskapssystemet må vedlikeholdes og revideres regelmessig. Sikringstiltakene som er planlagt bør regelmessig gjennomgås for å kontrollere at de fungerer som de skal.

Dersom det skjer endringer i forutsetningene for beredskapssystemet, bør dette følges opp i så snart som mulig. Eksempler på faktorer som kan kreve endringer er:

- Endringer i organisasjonsstrukturen
- Fysiske endringer (flytting, utbygging av kontorlokaler, oppussing)
- Endringer i trusselbildet

Store endringer kan medføre behov for å utarbeide en ny sikringsrisikoanalyse og legge denne til grunn for en større revisjon av beredskapssystemet. Det anbefales uansett å gjennomføre en sikringsrisikoanalyse med jevne mellomrom.

3.6 EKSEMPEL PÅ BRUK AV TILTAK I DE ULIKE BEREDSKAPSTRINN

Under er et eksempel på innføring av tiltak på ulike beredskapsnivåer. Alle tiltakene vil ikke være like relevante for alle virksomheter. Virksomhetene må selv bestemme hvilke tiltak som er hensiktsmessige og hvorvidt de må suppleres med andre tiltak. Det kan enten benyttes et sett med tiltak som knyttes opp mot et gitt beredskapsnivå, eller man kan velge ulike tiltak basert på den aktuelle trusselen.

TILTAK	BEREDSKAPSNIVÅ 1	2	3	4
A	Alle ansatte må vurdere egne aktivitetsmønstre og endre disse regelmessig	Møtevirksomhet med ekstern deltagelse reduseres til minimum	Kun ansatte får adgang til virksomheten	Kun ansatte med funksjoner definert som «kritiske» får adgang til virksomheten
B	Adgangskort må bæres synlig	Bruk av pinkode innføres på elektroniske låssystemer	Ansatte får adgang kun til områder der de har tjenstlig behov	Ingen endring
C	Iverksette kontroll av alle innpasserende kjøretøy	Iverksette kontroll av alle parkerte kjøretøy på virksomhetens område	Ingen kjøretøy tillates parkert nærmere enn 25 meter fra hovedkontoret	Ingen kjøretøy får kjøre inn på virksomhetens område
D	Gjennomgå rutiner for mottak av post og varer	All post og varer skal gå til post- og varemottak for kontroll	Varer fra ukjente avsendere avvises	Ingen endring
E	Sørge for at det er ryddig og oversiktlig	Fjern søppelkasser fra bygninger som er i bruk	Ingen endring	Ingen endring
F	osv ...	...	...	...

4

Anbefalt videre lesning

ASIS International (2008)
Threat Advisory System Response Guideline
Alexandria: ASIS International

ASIS International (2012)
Protection of assets: Physical Security
Alexandria: ASIS International

ASIS International (2012)
Protection of assets: Security Management
Alexandria: ASIS International

Forsvarsdepartementet (2007)
Ot.prp. nr. 21 (2007-2008) Om lov om endring i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven)
Oslo: Forsvarsdepartementet

Justis- og politidepartementet (2000)
Ot.prp. nr. 29 (2000-2001) Om lov om endringer i politiloven (overvåkingstjenestens oppgaver mv.)
Oslo: Justis- og politidepartementet

Justis- og politidepartementet (2008)
Meld. St. 22 (2007-2008): Samfunnssikkerhet – Samvirke og samordning
Oslo: Justis- og politidepartementet

Justis- og beredskapsdepartementet (2011)
Meld. St. 29 (2011-2012): Samfunnssikkerhet
Oslo: Justis- og beredskapsdepartementet

Justis- og beredskapsdepartementet (2013)
Meld. St. 21 (2012-2013): Terrorberedskap – Oppfølging av NOU 2012: 14 Rapport fra 22. juli-kommisjonen
Oslo: Justis- og beredskapsdepartementet

Forsvarsbygg (2005)
Sikringshåndboka – Håndbok i sikring og beskyttelse av eiendom, bygg og anlegg mot terrorhandlinger, spionasje, sabotasje og annen kriminalitet
Oslo: Forsvarsbygg (unntatt offentlighet)

Nasjonal sikkerhetsmyndighet (2015)
Veileder i sikkerhetsstyring
Kolsås: Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (2011)
Veiledning i objektsikkerhetsforskriften
Kolsås: Nasjonal sikkerhetsmyndighet.

Nasjonal sikkerhetsmyndighet (2009)
Veiledning i verdivurdering
Kolsås: Nasjonal sikkerhetsmyndighet.

Norges offentlige utredninger (NOU) (2006)
Når sikkerheten er viktigst – beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner
Oslo: Departementenes servicesenter

Norges offentlige utredninger (NOU) (2012)
Rapport fra 22. juli-kommisjonen
Oslo: Departementenes servicesenter

Norges offentlige utredninger (NOU) (2013)
Når det virkelig gjelder... – Effektiv organisering av statlige forsterkningsressurser
Oslo: Departementenes servicesenter

Omand, David, (2010)
Securing the State
London: Hurst & Co

Politidirektoratet (2007)
Politiets beredskapssystem del I – Håndbok i krisehåndtering
Oslo: Politidirektoratet

Standard Norge (2012)
Norsk standard 5830 – Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi
Oslo: Standard Norge

Standard Norge (2014)
Norsk standard 5831 – Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikostyring
Oslo: Standard Norge

Standard Norge (2014)
Norsk standard 5832 – Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse
Oslo: Standard Norge

A

Vedlegg A: Eksempler på sikringstiltak – virksomhet

Dette vedlegget gir eksempler på generelle grunnsikringstiltak og hensiktsmessige påbygningstiltak på virksomhetsnivå. Eksemplene er ikke uttømmende. Mange av tiltakene er generiske og kan innføres i større eller mindre grad, og vil være aktuelle på flere beredskapsnivåer. Eksempelvis er «å forsterke adgangskontrollen» et tiltak som kan innføres på et lavt beredskapsnivå og så styrkes ytterligere for hvert av de neste nivåene.

Eksemplene skiller ikke mellom *forebyggende* og *skadereduserende* tiltak. Når virksomheten velger tiltak er det imidlertid viktig å være bevisst på om tiltaket er forebyggende, skadereduserende eller begge deler. Bruk av eksempelvis splintreduserende vindusfilm forhindrer ikke at bomber benyttes i en terrorhandling, men er skadereduserende.

Sikringstiltakene i dette vedlegget omhandler hovedsakelig organisatoriske og menneskelige tiltak. Teknologiske tiltak, som for eksempel et adgangskontrollsystem, vil i mange tilfeller allerede være en del av grunnsikringen. Bruken vil imidlertid kunne skjerpes inn som følge av organisatoriske beredskapstiltak når høyere beredskapsnivåer innføres. Vær bevisst på bruk av påbygningstiltak og varigheten (livssyklusen) til disse.

Vedlegg A1
Adgangskontroll for personell og besøkende

TERRORSIKRING
En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015)

UTGITT AV
NASJONAL SIKKERHETSMYNDIGHET
POLITIDIREKTORATET
POLITIETS SIKKERHETSTJENESTE

Forsterket adgangskontroll for personell og besøkende kan redusere mulighetene for at mulige trusselaktører får adgang til bygninger/lokaler eller nærliggende områder.

Vurder inngangsområdet:
- Fysiske sperringer for å hindre ferdsel, spesielt fra gaten og inn til resepsjonsområdet
- Hvor mange adgangspunkter er det behov for?
- Kan forskjellige adgangspunkter varieres for å vanskeliggjøre eventuelle anslag?
- Kan adgangskontroll/inngang plasseres bort fra områder som ligger nær oppholdssted (kantine, oppholdsrom o.l.) for ansatte?

Vurder adgangskontrollen:
- Foreta kontroll av besøkende utenfor ordinært mottaks- og resepsjonsområde
- Identifiser alle personer som kommer inn i virksomheten ved å kontrollere legitimasjon, og oppbevar denne i resepsjon så lenge den besøkende oppholder seg på området
- Registrer besøkende (besøkslogg)
- Gjennomfør stikkprøvekontroller av håndbagasje for besøkende/ansatte. Den som ikke samtykker til kontroll, nektes adgang til virksomhetens område
- Begrens besøkendes adgang til områder og lokaler
- Ledsag besøkende
- Gjør besøkende kjent med endringen i besøksrutinene og hvilke praktiske følger dette får for dem

Vurder administrative tiltak:
- Kontroller låssystemer og foreta hyppige skifte av adgangskoder
- Aktiver forhåndsinnstilte adgangstilganger i henhold til beredskapsnivået: f.eks. hvilke dører som sperres, hvilke adganger som gis eller fjernes og hvor kode må tastes i tillegg til kort
- Orienter ansatte om bruk av panikk-kode i tillegg til normal PIN-kode på adgangskort. Bruk av panikk-kode bør øves for å sikre effekt i en reell situasjon
- Lås eller sperr av bygninger og områder som ikke er i regelmessig bruk

Vedlegg A2
Adgangskontroll for kjøretøy

TERRORSIKRING
En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015)

UTGITT AV
NASJONAL SIKKERHETSMYNDIGHET
POLITIDIREKTORATET
POLITIETS SIKKERHETSTJENESTE

Adgangskontroll med kjøretøy kan redusere muligheten for at kjøretøyer blir brukt til å aksjonere mot bygninger eller å skjule gjenstander, for eksempel sprenglegemer. Kjøretøyet i seg selv kan også brukes til å skade eller ødelegge. Vaktpersonell alene vil ikke kunne hindre et kjøretøy.

Vurder inngangsområdet:
- Iverksett robuste og effektive fysiske sperringer for å kontrollere ferdsel og hindre uvedkommende kjøretøyer adgang
- Etabler hindringer (sjikaner) for å redusere kjøretøyenes fart

Vurder kontrollen med kjøretøy:
- Iverksett eller styrke kontroller ved inn- og utkjørsler med vaktpersonell
- Gjennomgå virksomhetens innpasserings- og parkeringstillatelser og eventuell bruk av underjordisk parkeringsanlegg
- Fastsett en minste avstand mellom bygninger og parkerte kjøretøyer som kan brukes til å skjule sprenglegemer, så langt unna som praktisk mulig

Vurder skjerpede tiltak med virksomhetens egen transport:
- Sikre at kjøretøyer ikke forlates ulåst, og at de undersøkes før bruk
- Iverksett tiltak for å sikre virksomhetens kjøretøyer når de er parkert, særlig på offentlig område
- Undersøk kjøretøyer som har blitt forlatt ubevoktet før de tas i bruk
- Vokt virksomhetens kjøretøyer når de ikke befinner seg i et beskyttet og kontrollert område
- Kontroller passasjerer og bagasje ved egen transport av ansatte og ivareta sikkerheten ved av- og påstigningsplasser

Vedlegg A3
Post- og varemottak

TERRORSIKRING
En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015)

UTGITT AV
NASJONAL SIKKERHETSMYNDIGHET
POLITIDIREKTORATET
POLITIETS SIKKERHETSTJENESTE

Kontroll av brev- og pakkeforsendinger kan avdekke eksplosiver og brannstiftende, kjemiske, biologiske eller radioaktive midler.

- **Vurder eget mottaksområde for post og varer**

- **Vurder tiltak ved post- og varemottaksområdet:**
  - Etabler post- og varemottak et annet sted enn på virksomhetens område. Flere virksomheter kan gå sammen om dette for å spare kostnader
  - Installer eget ventilasjonsanlegg for mottaksområdet som er uavhengig av det øvrige anlegget. Dersom det er et felles ventilasjonsanlegg, ha rutine for å stenge dette umiddelbart ved funn av mistenkelig sending
  - Øk bruk av deteksjonsmidler

- **Vurder tiltak for mottak av post og varer:**
  - Alle vareleveranser skal gå til post- og varemottak, også kurersendinger og personlig adressert post
  - Avvise vareleveranser fra ukjente avsendere
  - Gjøre leverandører av varer og tjenester kjent med endringen i mottaksrutiner, og hvilke praktiske følger dette får for dem

Vedlegg A4
Fysiske omgivelser

TERRORSIKRING
En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015)

UTGITT AV
NASJONAL SIKKERHETSMYNDIGHET
POLITIDIREKTORATET
POLITIETS SIKKERHETSTJENESTE

Tiltak i de fysiske omgivelsene kan vanskeliggjøre utførelsen av anslag mot virksomhetens bygningsmasse og personell.

Vurder bygningsmassen:
- Påse at dører og vinduer er i god stand og at låse-/lukkerutiner blir fulgt
- Sjekk at eventuell splintfilm på vinduene er i tilfredsstillende stand
- Intensiver bruken av elektronisk overvåking av fysiske områder

Vurder uteområde/perimeter:
- Øk bruken av utvendig belysning
- Flytt unna alle gjenstander som kan brukes til å skjule sprenglegemer (for eksempel søppeldunker og kasser) fra bygninger/lokaler som er i bruk. Alternativt sikre slike punkter og plassere dem på overvåkede steder
- Benytt gjennomsiktige avfallssekker for lettere å kunne identifisere mistenkelige gjenstander
- Hold det ryddig og oversiktlig rundt virksomheten. Kutt ned og trim vegetasjon om nødvendig

Vurder fysisk sikring og vakttjeneste:
- Bruk bærbar alarm for vakt og resepsjon
- Øk visuell kontroll med parkerte kjøretøyer i virksomhetens nærhet
- Iverksett midlertidig parkerings- eller ferdselsforbud i samarbeid med politiet eller kommunen

Vedlegg A5
Personell

TERRORSIKRING
En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015)

UTGITT AV
NASJONAL SIKKERHETSMYNDIGHET
POLITIDIREKTORATET
POLITIETS SIKKERHETSTJENESTE

Ulike tiltak kan iverksettes for å vanskeliggjøre anslag mot personell og redusere skade på liv og helse.

Vurder hvilke tiltak som kan gjennomføres ved selve bygningsmassen:
- Flytt oppholds- og spiserom vekk fra innganger og resepsjonspartier
- Klargjør eventuelle forsterkede rom (retrettrom) for personell i spesielt utsatte funksjoner med beskyttelsesbehov
- Reduser eller unngå opphold i de delene av områder og bygninger som er mest sårbare for anslag

Vurder tilpasning av aktiviteter:
- Avlys aktiviteter som kan øke eksponeringen av ansatte eller lokalene
- Sørg for at ansatte varierer aktivitetsmønstre for å unngå å fremstå som et forutsigbart mål
- Påse at ansatte ikke samler seg i større grupper, når dette er mulig

Gi informasjon om situasjonen til de ansatte:
- Sørg for at de ansatte er kjent med beredskapsnivået og iverksatte tiltak
- Informer alle ansatte om trusselen fra terrorisme og hvilke former trusselen kan ta
- Påminn ansatte om å være årvåkne med hensyn til ukjente personer, kjøretøyer, etterlatte pakker og vesker, nettaktivitet og annen unormal aktivitet

Vurder personellets tilstedeværelse:
- Ansatte med en beredskapsfunksjon skal være tilgjengelige. Vurder å inndra ferier, permisjoner og avlyse tjenestereiser
- Vurder om andre ansatte uten beredskapsfunksjon ikke skal møte på jobb

Gjennomfør øvelser og evakueringsdriller:
- Sørg for at alle ansatte vet hva de skal gjøre dersom det inntreffer en hendelse

Vedlegg A6
Handling ved mottak av bombe- og terrortrussel

TERRORSIKRING
En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015)

UTGITT AV
NASJONAL SIKKERHETSMYNDIGHET
POLITIDIREKTORATET
POLITIETS SIKKERHETSTJENESTE

For å håndtere en mottatt trussel på best mulig måte, bør man få mest mulig informasjon for å hindre tap av menneskeliv og materiell skade.

- **Bombe- og terrortrusler fremsettes ofte over telefon og disse skal alltid tas på alvor**

- **Sentralbord, forkontor, resepsjoner, samt presse- og informasjonstjenester i alle virksomheter bør som del av beredskapstreningen være kjent med hva de gjør ved en innringt trussel**

- **Dersom du mottar en bombetrussel ved din virksomhet:**
  - Opptre rolig, vær vennlig og la innringeren få snakke uavbrutt
  - Slå på opptak dersom dette er tilgjengelig. Dersom det ikke er tilgjengelig, ta notater og få med deg mest mulig informasjon

- **Ved bombetrussel kan følgende spørsmål stilles når innringer har snakket ferdig:**

Når skal bomben eksplodere?
Hvor er bomben plassert?
Hvordan ser bomben ut?
Hvordan utløses bomben?
Hva slags sprengstoff og hvilken mengde er benyttet?
Hvem er du og hvorfor gjøres dette?

- **Noter:**
  - Tidspunktet trusselen ble mottatt
  - Lengden på samtalen
  - Hvilket nummer det ble ringt fra
  - Hvilket nummer det ble ringt til
  - Hvilken dialekt eller aksent som ble brukt
  - Hvilken sinnsstemning (opphisset, beruset, rolig) innringeren var i
  - Hvilket kjønn innringeren har
  - Hvilke lyder som er i bakgrunnen

- **Varsle umiddelbart nærmeste leder og sikkerhetsleder (som varsler politiet og vurderer å iverksette søk)**

Vedlegg A7
Evakuering ved bombe- og terrortrussel

TERRORSIKRING
En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015)

UTGITT AV
NASJONAL SIKKERHETSMYNDIGHET
POLITIDIREKTORATET
POLITIETS SIKKERHETSTJENESTE

- **Informer nødetatene om hvilken handlingsplan dere velger**

GJENNOMFØR ALTERNATIV EVAKUERING VED:

- **Brann:**
  - Dersom man mistenker en overlagt handling, bruk alternativ oppsamlingsplass
  - Alt personell skal kjenne til minst to utganger ved evakuering

- **Bombetrussel:**
  - Vurder full eller delvis evakuering
  - Ved mottak av brevbombe, evakuer rommet/etasjen, samt to etasjer opp og ned
  - Vurder om det er hensiktsmessig å forlate bygningen
  - Er bomben utenfor, kan det være hensiktsmessig å oppholde seg et sikkert sted i bygningen. Dette er gjerne områder uten vinduer, slik som trapperom, og bort fra dører, skillevinduer og ytre vegger
  - Unngå opphold på gateplan og første etasje om man velger å bli i bygget

- **Væpnet angrep:**
  - Ved væpnet angrep er det egne rutiner (se egen tiltaksliste)

- **Kjemisk/biologisk/radiologisk angrep:**
  - Hold personell igjen på området. Dersom noen er smittet, vil man få ytterligere spredning av smittemateriale. La personellet bli igjen til de kan bli undersøkt av medisinsk personell
  - Steng av ventilasjonen, lukk dører og vinduer

- **Alternativ oppsamlingsplass bør ikke være den samme som ved brann. Gjennomfør søk på alternativ plass før personellet samles. Unngå bruk av parkeringsplasser som oppsamlingsplass og hold alternativ oppsamlingsplass ved terrorhendelse helst 500 meter fra virksomheten**

- **Alternativ evakuering må øves**

Vedlegg A8
Rutiner for søk og funn

TERRORSIKRING
En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015)

UTGITT AV
NASJONAL SIKKERHETSMYNDIGHET
POLITIDIREKTORATET
POLITIETS SIKKERHETSTJENESTE

Rutiner for søk retter seg mot sabotasje mot de grunnleggende sikringstiltakene, mulige sprenglegemer eller bomber, forsøk på eller forberedelse til inntrengning og andre sikkerhetsmessige avvik. Personell som utfører søk bør være noen som kjenner virksomheten.

Rutiner for søk bør være utarbeidet som del av beredskapsplanverket:

- Søk bør gjennomføres ved økt terrorberedskap, etter en konkret trussel og etter en evakuering. Gjennomfør jevnlig søk ved endring i trusselen
- Personellet som gjennomfører søket trenger ikke kjenne til eksplosiver eller lignende, men må være kjent med området de søker for å kunne identifisere mulige trusler og ting som ikke hører til på området
- Søkspersonell bør arbeide i par for å gjennomføre søket så grundig og metodisk som mulig, og de bør ha forhåndsskrevne sjekklister

Ved iverksetting og gjennomføring av søk:

- Sikkerhetsleder bør tilkalle søkspersonellet enten gjennom telefon/tekstmelding eller gjennom en kodet beskjed over interne høyttaleranlegg
- Tildel søksområder til personell som kjenner områdene
- Gjennomfør søket diskret for ikke å uroe besøkende eller kunder
- Søk områder med allmenn tilgang som for eksempel garderober, toaletter, evakueringsveier, trapperom, innganger, korridorer, heiser, parkeringsplasser, varemottak og evakuerings- og brannoppsamlingsplasser

Ved funn av mistenkelig gjenstand:

- Varsle sikkerhetsleder
- Ikke ta på eller rør den mistenkelige gjenstanden
- Evakuer alle bort fra området og hindre at andre går frem til gjenstanden
- Informer kollegaer, gjester og kunder i området
- Den som har lokalisert den mistenkelige gjenstanden må være tilgjengelig for å informere politiet når de ankommer stedet
- Sikkerhetsleder bør konferere med politiet om evakueringsavstand og sikring av spor

Vedlegg A9
Informasjons- og kommunikasjonsteknologi (IKT)

TERRORSIKRING
En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015)

UTGITT AV
NASJONAL SIKKERHETSMYNDIGHET
POLITIDIREKTORATET
POLITIETS SIKKERHETSTJENESTE

Ingen beskyttelsestiltak blir effektive uten helhetlig sikring. Beskytt også dine vitale IKT-systemer mot mulige anslag.

- **Etabler vaktordning med nøkkelpersonell for å sikre drift av kritiske informasjonssystemer:**
  - Kontroller at tilgang til informasjonssystemene er mulig selv om nøkkelpersonell ikke er tilgjengelig
  - Sikre tilgang til systemdokumentasjon og passord for administratorer

- **Gjennomgå rutinene for:**
  - Sikkerhetskopiering og oppbevaring av sikkerhetskopiene
  - Gjenoppretting av sikkerhetskopier
  - Gjenoppretting av drift på alternativt sted med IKT-utstyr

Vedlegg A10
Krisekommunikasjon

TERRORSIKRING
En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015)

UTGITT AV
NASJONAL SIKKERHETSMYNDIGHET
POLITIDIREKTORATET
POLITIETS SIKKERHETSTJENESTE

En sikkerhetstruende hendelse vil føre til et behov for informasjon og kommunikasjon, noe som er essensielt for et effektivt samarbeid med både interne og eksterne samarbeidspartnere.

- **Kontroller rutinene for å motta og formidle instruksjoner fra politi, vaktstyrke og sikkerhetstjenester**
- **Kontroller aktuelle interne og eksterne varslingslister**
- **Kontakt leverandører og samarbeidende virksomheter for å bekrefte deres iverksettelse av tiltak i henhold til forhåndsavtale**
- **Sikkerhetskopier lister med kundekontakter, og om mulig oppbevar disse på et annet sted enn selve virksomheten**
- **Oppdater lister for pårørendekontakt**
- **Lag en strategi for eventuell mediahåndtering av saken**

B

Vedlegg B: Eksempler på sikringstiltak – individ

Dette vedlegget gir eksempler på generelle grunnsikringstiltak og hensiktsmessige påbygningstiltak på individnivå. Her gis noen eksempler på tiltak den enkelte medarbeider i virksomheten kan sette seg inn i og selv benytte. Eksemplene er ikke uttømmende. Noen av tiltakene er av generell art, mens andre tiltak er knyttet direkte til handling ved anslag.

Vedlegg B1
Tiltak for egenbeskyttelse

TERRORSIKRING
En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015)

UTGITT AV
NASJONAL SIKKERHETSMYNDIGHET
POLITIDIREKTORATET
POLITIETS SIKKERHETSTJENESTE

God sikkerhetskultur i en virksomhet vises i den enkelte medarbeiders adferd. På individuelt nivå er det enkelte tiltak man selv kan gjennomføre ved en skjerpet trusselsituasjon. Sett deg inn i retningslinjene for sikkerhet, vær oppmerksom på omgivelsene og bruk adgangstegn slik det er ment å brukes.

- **Bruk ID-kort når du oppholder deg inne på virksomheten. Skjul det når du er utenfor virksomheten**

- **Ikke slipp uvedkommende inn. Spør kollegaer/besøkende når de ikke har adgangstegn/ID-kort om hva de gjør på stedet**

- **Ikke la sensitive dokumenter ligge åpent og tilgjengelig. Vær oppmerksom på hva du kaster. Makuler sensitive dokumenter**

- **Ved skjerpet trussel – bruk huskeregel PIPPA for å sikre deg selv:**
  - **P**lan – tenk igjennom hva som kan skje ved en trussel og hva du vil gjøre
  - **I**nformasjon – pass på privat informasjon. Målutvelgelse skjer gjerne på internett
  - **P**rediksjon – ved skjerpet trussel, endre dine faste rutiner
  - **P**rofil – Ser du sårbar ut, er du muligens sårbar
  - **A**nonymitet – Skill mellom jobb og privatliv på informasjonen du gir ut om deg selv

- **Om du observerer noe som er merkelig – rapporter det**

Vedlegg B2
Handling ved væpnet angrep

TERRORSIKRING
En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015)

UTGITT AV
NASJONAL SIKKERHETSMYNDIGHET
POLITIDIREKTORATET
POLITIETS SIKKERHETSTJENESTE

Væpnet angrep er også omtalt som pågående livstruende vold (PLIVO). Et slikt angrep er ikke en gisselsituasjon, men en situasjon der én eller flere gjerningspersoner ønsker å påføre mest mulig skade og død.

- **Væpnet angrep kan skje med stikk-, slag- og skytevåpen, gjennomført av en eller flere personer**

- **Væpnet angrep kan skje plutselig og uten forvarsel. Slike angrep pågår oftest i mindre enn 15 minutter, eller inntil en væpnet respons stopper angrepet**

VED ET VÆPNET ANGREP:

- **LØP. Kom deg bort fra området. Dersom det er en skytter, og vedkommende ikke er i umiddelbar nærhet, løp for å komme deg i sikkerhet. Ikke ta med deg noe og hold hendene synlig. Advar andre**

- **SKJUL. Er du i nærheten av en skytter, barrikader deg, gjem deg og lås deg inne der det er mulighet. Sett telefonen på lydløs. Forhold deg rolig. Kom deg unna om du kan**

- **HANDLE. Rapporter når du har mulighet ved å ringe 112. Om du ikke kan snakke, la telefonlinjen ligge åpen slik at nødsentralen kan lytte**

- **Kun dersom du har mulighet til å gjøre det, *observer* og få med deg mest mulig informasjon om gjerningspersonen(e):**
  - Hvor mange?
  - Hvordan ser gjerningspersonen(e) ut/er gjerningspersonen(e) kledt?
  - Hvilke våpen har gjerningspersonen(e)? (f. eks. pistol, jaktrifle, hagle, automatgevær, kniv eller øks)
  - Hvor gikk gjerningspersonen(e)?
  - Hvor så du gjerningspersonen(e) sist og når?

- **Dersom du observerer på overvåkningskamera, rapporter fortløpende til nødnummer**

- **Ikke møt på brannoppsamlingsplass – kom deg i skjul, også utenfor bygget**
  - Skjul og dekning er ikke alltid det samme: Husk at ut av syne ikke betyr at du ikke kan rammes av skudd

- **Dersom du ikke har annet valg, og *kun da*, angrip gjerningspersonen når vedkommende er kommet til deg – det står om livet**

I MØTE MED VÆPNET RESPONS/POLITI:

- **Forhold deg rolig og vær klar over at du kan bli pekt på med våpen**

- **Væpnet respons er ikke der for å yte førstehjelp, de er der for å stoppe gjerningspersonen(e)**

- **Hold hendene dine synlig**

- **Følg instruksjonene deres og gi dem den informasjonen de trenger – har du sett gjerningspersonen(e), si ifra**

DESIGN: REDINK

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

Tlf. 67 86 40 00
post@nsm.stat.no
www.nsm.stat.no

POLITIDIREKTORATET

Postboks 8051 Dep, 0031 Oslo

Tlf. 23 36 41 00
politidirektoratet@politiet.no
www.politiet.no

POLITIETS SIKKERHETSTJENESTE

Postboks 4773 Nydalen, 0421 Oslo

Tlf. 23 30 50 00
post.pst@politiet.no
www.pst.politiet.no