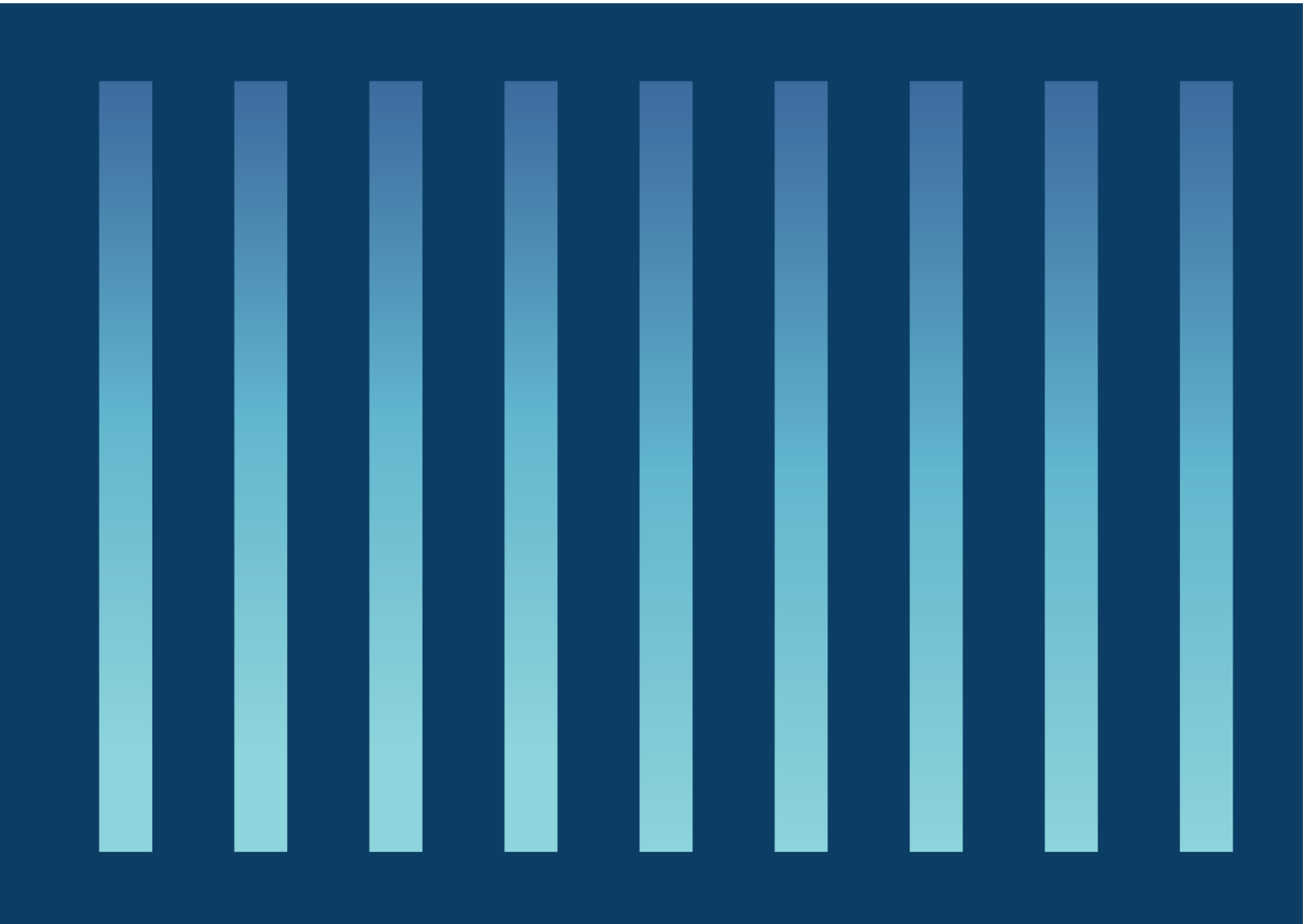
NASJONAL
SIKKERHETSMYNDIGHET

Grunnprinsipper for fysisk sikkerhet

Versjon: 1



INNHOLDSFORTEGNELSE

Introduksjon **3**
1. Identifisere og kartlegge **6**
1.1. Kartlegg virksomhetens verdier 6
1.2. Kjenn til trusselbildet 6
1.3. Kartlegg virksomhetens sårbarheter 7
1.4. Utfør en risikovurdering 7
1.5. Kartlegg utforming av sikkerhetstiltak 8
1.6. Planlegge og prosjektere 8
2. Beskytte **10**
2.1. Balansert sikring 10
2.1.1. Sikkerhetspreg 11
2.1.2. Barrierer 11
2.1.3. Deteksjon 12
2.1.4. Håndtere 13
2.2. Helhetlig sikring 13
2.2.1. Elektroniske 14
2.2.2. Menneskelige 14
2.2.3. Organisatoriske 15
2.3 Utføre øvelser 16
3. Opprettholde og oppdage **17**
3.1. Vedlikeholde 17
3.2. Kontrollere de fysiske sikkerhetstiltakene 17
3.3. Opprettholde gode endringsrutiner 18
4. Håndtere og gjenopprette **19**
4.1. Håndtere hendelser 19
4.2. Gjenopprette sikkerhetsnivå 19
4.3. Evaluere hendelsen 20
4.4. Lær av erfaringer og implementer forbedringer 20

Introduksjon

Globale sikkerhetspolitiske endringer preger samfunnsutviklingen også i Norge. Økende digitalisering, ny teknologi og politiske spenninger verden over medfører nye og komplekse utfordringer for samfunnssikkerheten.

Truslene Norge står overfor og trusselaktørenes interesser er dynamiske og rettet mot et bredt spekter av sektorer og virksomheter. NSM ser at trusselaktører benytter mer avanserte metoder enn tidligere, og risiko- og sårbarhetsbildet er blitt mer avansert. Aktørenes evne og vilje, sammen med deres måte å operere på, er dimensjonerende for hvordan nasjonen, virksomheter og individer må sikre sine verdier. I møte med disse utfordringene må rammer og krav defineres og tydeliggjøres for virksomheters arbeid med forebyggende sikkerhet, gjennom både redusering av sårbarheter og håndtering av sikkerhetstruende virksomhet.

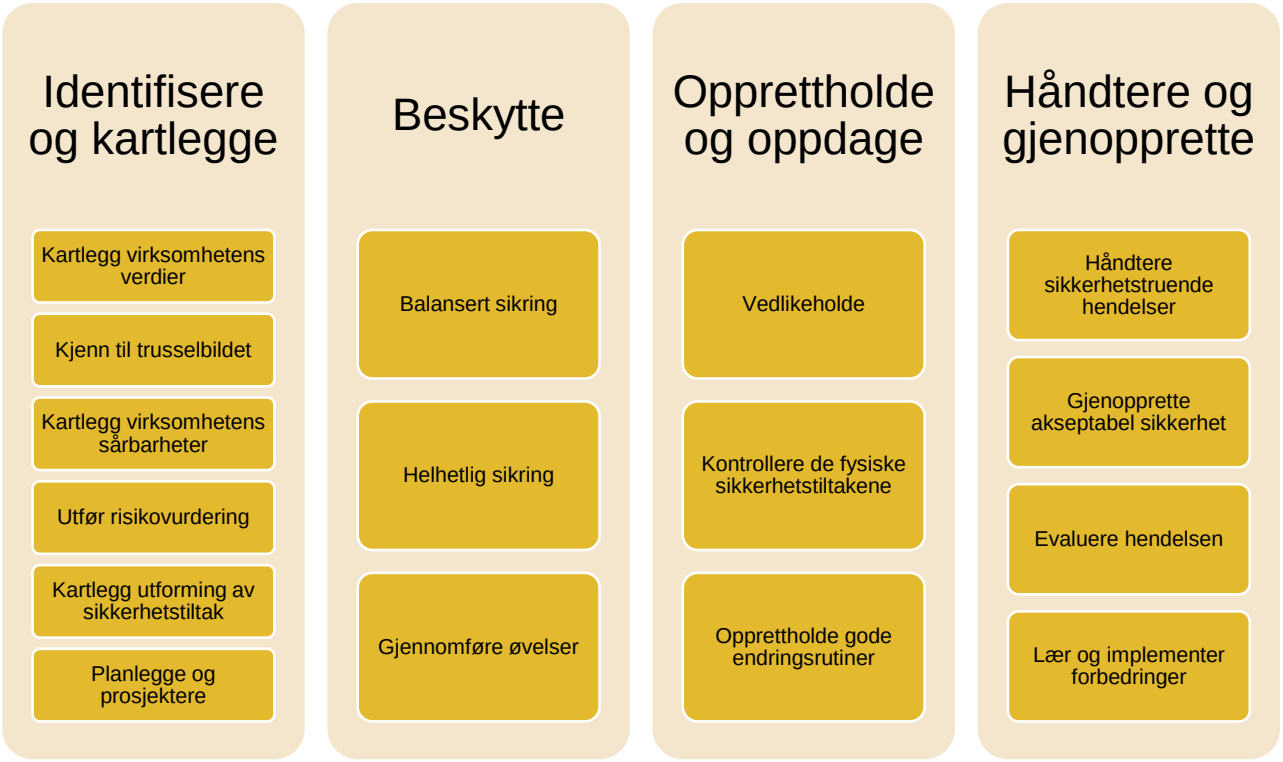
Virksomheter som skal etablere sikkerhetstiltak for å beskytte sine verdier må ha forståelse og overblikk for risikobildet de står ovenfor. Risikovurderinger gjør en virksomhet i stand til å identifisere hvordan de best kan beskytte verdiene virksomheten forvalter gjennom risikoreduserende tiltak. For å ivareta sikkerhetsarbeidet må virksomheten bl.a. identifisere hvilke verdier virksomheten råder over, analysere risiko for at verdiene kan gå tapt, og iverksette og opprettholde nødvendige tiltak slik at verdiene er tilstrekkelig beskyttet.

Det er derfor viktig at virksomheten etablerer og opprettholder et sikkerhetsstyringssystem som kontinuerlig følger opp aktivitetene med betydning for sikkerhetstilstanden til virksomheten (se veileder i sikkerhetsstyring og NSMs grunnprinsipper for sikkerhetsstyring for mer informasjon).

Det er viktig at virksomheter ser helhetlig på sikkerhetstilstanden slik at de kan etablere de tiltakene som er mest hensiktsmessige, innenfor fysisk, personell og IKT-sikkerhet. Etablering av slike tiltak kan være kostbart og tidskrevende og blir ofte nedprioritert i en virksomhet. Der innførte sikkerhetstiltak ikke har forventet eller planlagt effekt, og f.eks. fysiske og digitale tiltak ikke ses i sammenheng, vil ikke virksomheter kunne oppnå helhetlig sikring.

Fysiske sikkerhetstiltak skal bidra til å forhindre, avdekke og forsinke et sikkerhetstruende hendelsesforløp. Tiltakene bør bestå av en kombinasjon av barrierer, deteksjon, verifikasjon og reaksjon som er tilpasset behovet for beskyttelse av verdiene.

NSMs grunnprinsipper i fysisk sikkerhet har som hensikt å bidra til virksomheters arbeid med forebyggende sikkerhet og etablering av fysiske sikkerhetstiltak. Grunnprinsippene er ikke knyttet opp mot krav i, eller i medhold av sikkerhetsloven eller andre regelverk. For virksomheter underlagt sikkerhetsloven viser vi til NSMs *Veileder i fysisk sikkerhet,* der det dannes et grunnlag for virksomhetenes arbeid med å etterleve regelverket. Virksomheten har et selvstendig ansvar for å vurdere om det er juridiske begrensinger innenfor dens virkeområde som vil sette enkelte tiltak til side.



Hva er NSMs grunnprinsipper for fysisk sikkerhet?

NSMs grunnprinsipper for fysisk sikkerhet definerer et sett med prinsipper med fokus på det fysiske aspektet ved å forebygge, oppdage og håndtere sikkerhetstruende virksomhet. Dette er prinsipper og underliggende anbefalinger som skal bidra i virksomhetens arbeid med å beskytte verdier og funksjoner mot uautorisert adgang, inntrengning, skade eller tap. Prinsippene forklarer hva en virksomhet bør gjøre for å etablere og opprettholde fysisk sikkerhet og hvorfor dette arbeidet bør gjøres. Derimot forklarer det ikke virksomheten hvordan det skal utføres. Valg av tiltak bør baseres på virksomhetens egne behov, muligheter og begrensninger.

Grunnprinsippene er ikke ment å være enkeltstående prinsipper, men bør sees i sammenheng med virksomhetens helhetlige sikkerhetsstyringsarbeid. Virksomheter vil først kunne oppnå et akseptabelt sikkerhetsnivå når de har identifisert og implementert tiltak som ivaretar det organisatoriske, elektroniske, fysiske og menneskelige aspektet. Kombinasjonen av disse tiltakene danner grunnlag for helhetlig sikring.

Grunnprinsipper i fysisk sikkerhet er delt inn i følgende kategorier:

1. Identifisere og kartlegge
2. Beskytte
3. Opprettholde og oppdage
4. Håndtere og gjenopprette

Hvert grunnprinsipp inneholder anbefalinger som beskriver hva virksomheten bør gjøre. Listene over anbefalinger er ikke uttømmende. Flere av grunnprinsippene henger sammen og enkelte er en

forutsetning for å kunne implementere andre grunnprinsipper på en god måte. Grunnprinsippene i fysisk sikkerhet inkluderer sikringstiltak som består av barrierer, deteksjon, verifikasjon og reaksjon for å etablere god sikkerhet i dybden. Tiltakene gjelder for både utilsiktede og tilsiktede handlinger, men hovedfokuset har vært tilsiktede handlinger.

Grunnprinsipper for fysisk sikkerhet skal bistå virksomheter med å utarbeide hensiktsmessige fysiske sikkerhetstiltak. Hovedfokuset er hva virksomheter kan gjøre for å forebygge, oppdage og håndtere sikkerhetstruende virksomhet ved bruk av fysiske sikkerhetstiltak.

Målgruppe

Grunnprinsippene er sektorovergripende og gir anbefalinger for alle virksomheter som ønsker å beskytte verdiene sine. Prinsippene er relevante for en stor variasjon av virksomheter og kan også være et godt utgangspunkt for virksomheter underlagt sikkerhetsloven.

Målgruppen for grunnprinsippene er primært sikkerhetsledere og andre med ansvar for den fysiske sikkerheten i en virksomhet. For å sikre at virksomheten har tilstrekkelig ressurser og kompetanse for å ivareta sikkerheten er det avgjørende at målene for sikkerhetsarbeidet forankres hos øverste ledelse. Samtidig er det viktig at utøvelsen av fysisk sikkerhet ivaretas i alle ledd – av den øverste ledelse, mellomledere og ikke minst medarbeiderne

1. Identifisere og kartlegge

Denne kategorien skal legge grunnlaget for en effektiv implementering av de øvrige grunnprinsippene. Dette er prinsipper for at virksomheten skal kartlegge og identifisere verdier de ønsker å beskytte, hva som kan ramme verdiene, nåværende sikkerhetstilstand og sårbarheter, hvilke forutsetninger som ligger til grunn og virksomhetens funksjonelle behov. På bakgrunn av dette utarbeides en plan for utforming av nødvendige fysiske sikkerhetstiltak. Kartlegging og identifisering av det fysiske må legges til grunn for utarbeidelse av en risikovurdering.

1.1. Kartlegg virksomhetens verdier

For å kunne vurdere risiko og hvilke fysiske risikoreduserende tiltak som bør implementeres, er det essensielt at virksomheten foretar en kartlegging av egne verdier. Virksomhetens verdier kan være objekter, informasjon, informasjonssystemer og infrastruktur.

Hvorfor er dette viktig: Kartlegging og identifisering av virksomhetens egne verdier gir viktig informasjon om hva en trusselaktør kan være ute etter.

Anbefalte tiltak:

- Identifiser virksomhetens verdier, både egne og de virksomheten råder over på vegne av andre
- Kartlegg plassering av verdier
- Kartlegg adkomstaksene til verdier

1.2. Kjenn til trusselbildet

Virksomheten bør ha kunnskap om det gjeldende trusselbildet og hva som kan ramme verdiene til virksomheten. Dette innebærer at virksomheten tilegner seg kunnskap om relevant trusselinformasjon for sin virksomhet. Virksomheten bør videre ha kjennskap til trusselaktørers evne og vilje og hvordan de kan operere for å forsere de fysiske sikkerhetstiltakene.

Hvorfor er dette viktig: For å kunne iverksette riktige tiltak, er det viktig at virksomheten gjør seg kjent med trusler og forliggende risiko som er gjeldende for virksomheten og dens verdier.

Anbefalte tiltak:

- Hent informasjon fra relevante fagorganer f.eks.:

    - PST
    - E-tjenesten
    - NSM
    - Sektordepartement
- Vurder trusselaktørens evne og vilje til å kunne skade eller påføre tap av verdier

1.3. Kartlegg virksomhetens sårbarheter

Kartlegging av virksomhetens fysiske sårbarheter innebærer å identifisere de fysiske forhold ved virksomheten som kan utnyttes av en trusselaktør. Dette kan være plassering av verdiene, lokasjonen til virksomheten, de omkringliggende områdene og virksomhetens avhengigheter.

Hvorfor er dette viktig: Kjennskap til virksomhetens sårbarheter vil øke muligheten for at de riktige og mest hensiktsmessige tiltakene med en reell risikoreduserende effekt blir valgt.

Anbefalte tiltak:

- Kartlegg virksomhetens sårbarheter som en del av risikovurderingen
    - Identifiser trusselaktørens mulighet til å påvirke, skade, ødelegge eller på annen måte påføre tap av verdier
- Identifiser avhengigheter som kan utnyttes av en trusselaktør f.eks.:
    - Strøm og vann
    - Kjøling
    - Kommunikasjon
    - Eksterne tjenester eksempelvis alarm, vakthold og andre leverandører

1.4. Utfør en risikovurdering

Basert på identifisering av verdier, trusler og sårbarheter, bør virksomheten utføre en risikovurdering. De fysiske sikkerhetstiltakene som skal beskytte virksomhetens verdier, opprettholde akseptabelt sikkerhetsnivå, oppdage og håndtere sikkerhetstruende virksomhet, skal velges og implementeres ut ifra virksomhetens risikovurdering.

Risikovurderingen kan med fordel etableres med grunnlag i anerkjente standarder for risikovurdering som for eksempel NS-ISO 31000:2018, NS 5832:2014 og NS 5814:2008.

Hvorfor er dette viktig: En risikovurdering er nødvendig for å kunne identifisere behovet for fysiske sikkerhetstiltak som bør implementeres for å redusere risiko og oppnå tilstrekkelig sikkerhet for virksomheten.

Anbefalte tiltak:

- Utfør en grundig risikovurdering
- Utfør risikovurderinger jevnlig og/ eller ved endringer i virksomheten f.eks. ved:

- Tilførte / endrede verdier
- Endringer i trusselbilde
- Avdekkede sårbarheter
- Ved sikkerhetstruende virksomhet

1.5. Kartlegg utforming av sikkerhetstiltak

Virksomheten bør kartlegge de nåværende fysiske sikkerhetstiltakene og identifisere hva som må til for å redusere risikoen til akseptabelt nivå. Ved å identifisere områder og funksjoner som er sårbare og innehar risiko, vil virksomheten kunne planlegge spesifikke fysiske tiltak som vil redusere risikoen forbundet med dette. Sikkerhetstiltakene bør utformes på en slik måte at de oppnår balansert sikring, dybde i sikringen og at tiltakene virker uavhengig av hverandre.

Hvorfor er dette viktig: Kartlegging av nåværende sikkerhetstiltak vil identifisere behovet for ulike fysiske sikkerhetstiltak for å redusere risikoen og øke mulighetene for deteksjon og reaksjon ved en sikkerhetstruende virksomhet.

Anbefalte tiltak:

- Kartlegg alle implementerte sikkerhetstiltak og evaluer om de gir ønsket effekt
- Identifiser sikkerhetstiltak som ikke fungerer og årsak til dette gjennom:
  - Avvik
  - Revisjon / tilsyn
  - Øvelse / trening
- Identifiser områder og funksjoner som har behov for økt fysisk sikkerhet
- Kartlegg behovet for avskrekkende, tidsforsinkende, skadebegrensende og detekterende sikkerhetstiltak og de mulige kombinasjonene som vil redusere risiko til akseptabelt nivå
  - Må sees i sammenheng med behovet for organisatoriske, menneskelige og elektroniske sikkerhetsbehov for å oppnå helhetlig sikring

1.6. Planlegge og prosjektere

Virksomheten bør etablere en plan for implementering av sikkerhetstiltak. Det er viktig at sikkerhetsarbeidet organiseres på egnet måte. Dette er uavhengig av om det skal foretas en revisjon av eksisterende sikkerhetstiltak, eller om virksomheten skal etablere tiltak for første gang.

På grunnlag av risikovurderingen som er utført bør virksomheten kartlegge de interne og eksterne krav som stilles til sikkerheten, og definere hvilke sikringsbehov virksomheten har. Disse kravene gir føringer for hvordan virksomheten skal oppnå sine sikringsmål. På bakgrunn av verdivurderingen vil virksomheten være i stand til å kunne definere trusler som er aktuelle og dermed definere beskyttelsesbehovet. Om verdiene er avhengig av at informasjonens konfidensialitet ikke blir kompromittert, kan virksomheten ha et større behov for tiltak som hindrer avlytting og innsyn enn tiltak mot terroranslag.

Virksomheter med ulik størrelse og ulike beskyttelsesbehov vil ha forskjellige tilnærminger til planlegging og prosjektering av sikkerhetstiltak.

Dette kan med fordel gjøres med grunnlag fra anerkjente standarder innen sikkerhet i byggeprosjekter som for eksempel NS 5834:2016 – Samfunnssikkerhet – beskyttelse mot tilsiktede uønskede handlinger – Planlegging av sikringstiltak i bygg, anlegg og eiendom.

Hvorfor er dette viktig: Virksomheter bør definere beskyttelsesbehovet for at implementeringen av planlagte sikkerhetstiltak skal fungere etter sin hensikt.

Anbefalte tiltak:

- Kartlegg interne og eksterne krav til sikkerhet
- Inkluder fagpersoner tidlig i planleggingsfasen
- Sørg for at virksomhetens beskyttelsesbehov setter føringer for valg som blir tatt
- Kartlegg lokasjon og omkringliggende områder som kan forringe sikkerheten
- Sørg for å ivareta konfidensialitetsbehov om nødvendig, også hos leverandører og eksterne samarbeidspartnere
- Sørge for at sikkerheten blir ivaretatt under anskaffelse av utstyr (se NSM grunnprinsipper for IKT-sikkerhet for mer informasjon)

2. Beskytte

Formålet med denne kategorien er å beskrive sikkerhetstiltakene som skal beskytte verdiene mot uautorisert tilgang, ødeleggelse, sabotasje, innsyn og avlytting. Virksomheten må selv velge strategi og utforming av tiltak for å effektivt kunne forebygge, detektere, forsinke og håndtere sikkerhetstruende virksomhet, og begrense skader på sine verdier. Ved valg av sikringsstrategi vil virksomheter kunne opprette tiltak som er hensiktsmessige og funksjonelle sett opp mot risikovurdering, krav og virksomhetens behov.

Tiltakene bør settes sammen slik at virksomheten oppnår helhetlig og balansert sikring. Dette gjøres ved å kombinere ulike tiltakskategorier for å forebygge, detektere, forsinke, håndtere og begrense skade. For å oppnå helhetlig sikring er man avhengig av at de fysiske, elektroniske, menneskelige og organisatoriske tiltakene fungerer sammen og understøtter hverandre. Virksomheten bør derfor gjennomføre øvelser for å kontrollere at tiltakene fungere som de skal og at de fungerer sammen.

2.1. Balansert sikring

Balansert sikring betyr at de etablerte fysiske sikringstiltakene virker sammen og selvstendig, og ikke motvirker hverandre. De enkelte tiltakene bør fungere uavhengig av hverandre slik at frafall av ett ikke påvirker den totale sikringsevnen. Tiltakene bør understøtte og ha en forsterkende effekt på hverandre. Dette kan oppnås gjennom forebyggende tiltak som juridiske barrierer, skilting og et tydelig sikkerhetspreg. Fysiske barrierer opprettes der det er behov for å fysisk hindre eller forsinke en trusselaktør. Barrierene bør understøttes av deteksjonsmidler i form av ulike sensorer som IR, termisk, kamera eller bevegelse. Deteksjonstiltakene skaper mulighet for rettidig og effektiv håndtering av identifisert trussel.

Ved å etablere flere lag med fysiske barrierer oppnår man sikring i dybden. Dette vil gjøre det vanskeligere og mer tidkrevende for en trusselaktør å få tilgang til verdien. Sikring i dybden oppnås blant annet gjennom tydelige autorisasjonskiller og soneinndeling.

For å planlegge, kontrollere og dokumentere effekten av de fysiske sikringstiltakene bør virksomheten utforme et estimert tidsforløp for en uønsket handling. Dette tidsforløpet blir ofte betegnet «tidsregnskap». Tidsregnskap regnes fra en hendelse detekteres og til et planlagt utfall av en sikkerhetstruende hendelse har funnet sted.

Tidsregnskap er en metode som gjør virksomhetene i stand til å kunne måle om effekten av sikkerhetstiltakene kan motvirke tap av verdiene som skal beskyttes. Dette bør estimeres for alle relevante scenarioer og identifiserte verdier.

2.1.1. Sikkerhetspreg

Virksomheten bør være bevisst hvilket sikkerhetspreg de ønsker og har behov for når de fysiske sikkerhetstiltakene utformes og etableres. Virksomheten kan oppnå ulik forebyggende effekt gjennom sin visuelle profil. Det kan være ønskelig å benytte skjulte tiltak for virksomheter med publikumskontakt, da skjulte tiltak ikke fremstår som skremmende for publikum. En annen fordel med skjulte tiltak er at det kan gjøre det vanskeligere for en trusselaktør å kartlegge tiltakene.

Ønsker virksomheten større grad av avskrekkende effekt kan dette gjøres ved å ha et tydelig sikkerhetspreg. Dette kan oppnås gjennom tydelig skilting, synlig vakthold, juridiske og fysiske barrierer. Et slikt tiltak kan ha stor effekt på «opportunisten» og kan derfor være med å forhindre lavterskelangrep. En trusselaktør med høyere grad av evne og vilje vil i mindre grad la seg avskrekke. Avskrekkende tiltak kan derimot være med å styre aktørens metode for inntrengning.

Hvorfor er dette viktig: Ved å være bevisst hvilket sikkerhetspreg virksomheten ønsker, kan tiltakene utformes slik at de ikke går på bekostning av virksomhetens overordnede mål og behov, samtidig som sikkerhetstiltakene fungerer etter hensikt.

Anbefalte tiltak:

- Integrer sikkerhetsmål og virksomhetsmål
- Sørg for at ønsket sikkerhetstilstand oppnås uavhengig av valgt sikkerhetspreg
- Skjulte tiltak
    - Integrer tiltakene i eksisterende omgivelser
    - Etabler klare autorisasjonsskiller
    - Tilstreb avstand fra publikum til verdiene
- Synlige tiltak
    - Bruk skilt for å tydeliggjøre juridisk grense og konsekvenser ved ulovlig inntrengning
    - Tydeliggjøre advarsler om etablerte sikkerhetstiltak (som vakthold med hund, vekter o.l.) på innsiden, og restriksjoner
    - Etabler andre synlige tiltak som er demotiverende for en aktør som f.eks.:
        - Gjerder
        - Kjøretøybarrierer
        - Synlig vakthold

2.1.2. Barrierer

Formålet med fysiske barrierer er å hindre og forsinke trusselaktøren tilstrekkelig før de kommer frem til verdiene slik at planlagt reaksjon kan iverksettes. De fysiske barrierene bør plasseres og utformes slik at de gir ønsket effekt mot identifisert trussel og er dimensjonert for verdien de er ment å beskytte. Plassering og utforming avhenger av om verdiene skal beskyttes mot ødeleggelse, sabotasje eller kompromittering.

Bruk av soneinndeling og opprettelse av sikre områder kan bidra til å øke inntrengningstiden til en trusselaktør. Soneinndeling, med gode autorisasjonsskiller og tilhørende sikringstiltak, skaper en

barriere rundt verdiene som er ønsket beskyttet. Soneinndelingen bør være hensiktsmessig utformet for å sikre funksjonalitet i kombinasjon med beskyttelse.

Fysiske barrierer kan med fordel utformes med grunnlag i anerkjente standarder som NS-EN 1627, som det også refereres til Sikringshåndboka til Forsvarsbygg. Disse gir et godt utgangspunkt for å planlegge etableringen av fysiske barrierer. Det er viktig å understreke at tiltakene etableres med utgangspunkt i virksomhetens risikovurdering.

Hvorfor er dette viktig: Uten tilstrekkelige barrierer vil virksomhetens verdier være sårbare mot skade, sabotasje eller kompromittering. Dimensjonering av fysiske barrierer vil gi virksomheten en forventing av hvor lang reaksjonstid som kan aksepteres.

Anbefalte tiltak:

- Plasser barrierer slik at de gir ønsket effekt
- Sørg for tilstrekkelig avstand mellom verdi og ytterste barriere
- Etabler fysiske barrierer i kombinasjon med soneinndeling/autorisasjonskiller
- Sørg for at barrierene understøttes av deteksjon og reaksjon
- Sørg for at barrierenes konstruksjon gir ønsket effekt mot identifisert trussel
- Sørg for at barrieren dimensjoners for verdien som skal beskyttes
- Etabler lagvis oppbygning av ulike barrierer som totalt gir ønsket sikkerhetsnivå og sikring i dybden

2.1.3. Deteksjon

Deteksjon av sikkerhetstruende virksomhet er i de fleste tilfeller en forutsetning for å kunne avverge eller begrense skade. Tidlig deteksjon gir mulighet for effektiv avverging og håndtering av sikkerhetstruende virksomhet. Når en hendelse blir detektert i tidlig fase vil avverging og implementering av tiltak øke mulighet for å begrense skade.

Virksomheter bør etablere deteksjonsmidler, for eksempel kamera med tilhørende sensorer som IR, termisk og bevegelse, alarmanlegg eller andre midler. Dette kan tidlig gi varsling om en pågående sikkerhetstruende hendelse. Kameraer og andre deteksjonsmidler bør plasseres på logiske steder for å kunne overvåke størst mulig område og ved adkomstaksene til verdiene som skal beskyttes.

Deteksjon av en hendelse må verifiseres for at riktig tiltak iverksettes. Om en alarm er utløst eller en hendelse er detektert vil en kunne verifisere om alarmen er reell og deretter iverksette riktig tiltak, varsle utrykningsstyrker samt varsle personell. Bruk av bevegelige kamera som kan styres fra en alarmsentral vil for eksempel gi muligheter for en tidlig deteksjon av hendelse og iverksettelse av tiltak.

Hvorfor er dette viktig: Tidlig deteksjon og verifikasjon gir virksomheter mulighet til å reagere på en hendelse så fort som mulig samt begrense skadeomfanget i tilstrekkelig grad.

Anbefalte tiltak:

- Etabler bemannet resepsjon og vaktsentral med kvalifisert personell
- Opprett perimetersikring med tilhørende sensor
- Opprett belysning av sikret områder
- Opprett mulighet for verifikasjon
    - Vaktstyrke
    - Kamera
    - Droner
- Sørg for rutiner for å oppdage annen sikkerhetstruende virksomhet som f.eks.:
    - Uønsket rekognosering av virksomheten
    - Rapportering om mistenkelig aktivitet fra ansatte

2.1.4. Håndtere

Virksomheten må kunne møte en pågående sikkerhetstruende hendelse med en respons. Dette kan oppnås gjennom aktive tiltak som alarm med kraftige sirener, strobelys og røykanlegg eller destruksjon av informasjon.

Avhengig av virksomhetens verdier, risikobilde og behov kan det være nødvendig med en avtale om bruk av reaksjonsstyrke. Dette kan være politi, sivile vaktstyrker eller militære sikringsstyrker. Virksomheten må være bevisst hvilken handlingsrom og juridiske begrensninger de ulike styrkene vil ha og hva som kan forventes av dem. En avtale om bruk av reaksjonsstyrker bør inkludere forventninger til hva reaksjonsstyrkenes oppgave er, responstid, hvordan en hendelse bør håndteres, hva som er viktig å beskytte for virksomheten og hvem som skal varsles ved en pågående sikkerhetstruende hendelse. Et slikt samarbeid bør øves jevnlig.

Hvorfor er dette viktig: Virksomheten bør ha tiltak for å kunne respondere på en pågående sikkerhetstruende hendelse og begrense skadene.

Anbefalte tiltak:

- Etabler skadebegrensende tiltak
    - Alarm med varsling
    - Evakuering
    - Nedlåsing
    - Destruksjon
- Sørg for avtale med reaksjonsstyrke

2.2. Helhetlig sikring

Uten et helhetlig perspektiv på sikkerhet vil det være vanskelig for virksomheten å oppnå et akseptabelt sikkerhetsnivå. Akseptabelt sikkerhetsnivå oppnås først når virksomheten har identifisert og implementert både fysiske, IKT-messige og personellmessige sikkerhetstiltak

Dette arbeidet starter med virksomhetens overordnede plan for sikringskonsept som er basert på risikovurderingen med identifisering av verdier, trusler, sårbarheter, inkludert konsekvens og sannsynlighet for sikkerhetstruende virksomhet.

Når virksomheten utarbeider sin plan for utforming av fysiske sikringstiltak bør dette gjøres i sammenheng med de menneskelige, elektroniske og organisatoriske sikkerhetstiltakene. Først når disse virker sammen og understøtter hverandre vil man kunne oppnå helhetlig sikring. Verdier med samme sikkerhetsbehov kan sikres ved å benytte ulike tiltak eller en kombinasjon av flere, såfremt de oppnår samme effekt. Dette betyr at de ovennevnte tiltakene må ha samme motstandskraft mot identifisert trussel. Sikkerheten blir aldri bedre enn det svakeste ledd.

2.2.1. Elektroniske

Elektroniske sikkerhetstiltak er tiltak som bruker elektrotekniske utstyr og løsninger for å støtte, supplere eller erstatte fysiske sikkerhetstiltak. Elektroniske barrierer kan være etablering av elektronisk adgangskontroll og TV- og videoovervåkning.

Ved å kombinere de fysiske tiltakene med elektroniske tiltak kan man oppnå en økt grad av beskyttelse da det enkelte fysiske tiltaket ikke nødvendigvis er nok for å beskytte verdien. Der et fysisk tiltak alene kun kan stanse eller forsinke en inntrenger, vil inkluderingen av elektroniske tiltak gi mulighet for deteksjon, alarm, verifikasjon og loggføring.

Der fysiske tiltak har blitt etablert understøttet av elektroniske tiltak er det viktig å være bevisst hvilke eventuelle nye sårbarheter dette kan medføre dersom systemene ikke understøtter hverandre på ønsket måte. Innføring av et elektronisk kortlesersystem gir mulighet for effektiv adgangskontroll. Det kan også tilføre nye sårbarheter dersom tilgangsstyringen på kortleseren ikke oppdateres jevnlig eller har svak IKT-sikkerhet.

Hvorfor er dette viktig: For at virksomheten skal kunne detektere sikkerhetstruende virksomhet bør elektroniske sikkerhetstiltak understøtte de fysiske.

Anbefalte tiltak:

- Opprett elektronisk adgangskontroll
- Opprett TV- og videoovervåkning
- Etabler sensor med tilhørende alarmsystem

2.2.2. Menneskelige

Menneskelige sikkerhetstiltak er ment å påvirke vurderingsevne, kunnskap, adferd og reell evne til å bruke øvrige sikkerhetstiltak. Tiltakene skal sørge for tilstrekkelig risiko- og sikkerhetsforståelse blant personell tilknyttet virksomheten.

Ved etablering av fysiske sikkerhetstiltak må de menneskelige tiltakene understøtte disse for å oppnå ønsket effekt. Det er en forutsetning at personell tilknyttet virksomheten har tilstrekkelig sikkerhetsforståelse slik at de fysiske sikkerhetstiltakene blir benyttet etter hensikt.

Etablerer virksomheten fysiske sikkerhetstiltak som oppleves uhensiktsmessige eller hindrer virksomhetens øvrige drift vil dette kunne resultere i at enkelte omgår eller manipulerer tiltaket.

Hvorfor er dette viktig: For at de fysiske sikkerhetstiltakene skal kunne virke etter sin hensikt må personell tilknyttet virksomheten ha tilstrekkelig kunnskap om disse for å sørge for at de fungerer som de skal, og ikke blir omgått eller manipulert. Se til NSMs temarapport *Innsiderisiko.*

Anbefalte tiltak:

- Sørg for tilstrekkelig kompetanse
- Opprett klare rutiner
- Sørg for at virksomheten har gode varslingsrutiner
- Sørg for tydelig kommunikasjon
- Sørg for sikkerhetsledelse

2.2.3. Organisatoriske

Organisatoriske barrierer er tiltak i form av skriftlige eller muntlige beskrivelser, vurderinger og beslutninger som regulerer ledelse, organisering, prosesser, analyser, adferd og/eller anvendelse av sikkerhetstiltak.

Organisatoriske barrierer kan etableres i form av skilting, opplæring og bruk av adgangskort for å understøtte de fysiske sikkerhetstiltakene.

Ved etablering av de fysiske sikkerhetstiltakene bør virksomheten være bevisst hvordan andre krav og bestemmelser påvirker utformingen av disse. Krav stilt i branninstrukser, arbeidsmiljølov og andre HMS bestemmelser bør integreres i utformingen av fysiske sikkerhetstiltak.

Hvorfor er dette viktig: Virksomheten må identifisere sine organisatoriske behov for å kunne få full effekt av de fysiske sikkerhetstiltakene.

Anbefalte tiltak:

- Opprett og kommuniser instrukser
- Etabler tydelig skilting
- Sørg for oppfølgning av HMS bestemmelser og arbeidsmiljøloven

2.3 Utføre øvelser

For å teste og kontrollere de etablerte sikkerhetstiltakene bør virksomheten utføre øvelser for å kontrollere at disse fungerer som forventet. Dette vil også kunne teste hvordan personell responderer på de ulike tiltakene. Øvelser i virksomheten kan gjennomføres ved å spille ut hele scenarioer (fullskala) som inkluderer inntrenging, spionasje, sabotasje, terror eller subversjon, funksjonsøvelse hvor enkelte funksjoner i virksomheten øves, eller gjennom diskusjonsøvelser hvor man går igjennom planverk, handlingsplaner etc. Alle parter som kan bli berørt ved faktisk sikkerhetstruende hendelse bør involveres slik at alle roller og funksjoner blir testet. Fullskala øvelser bør utføres så realistiske som mulig hvor personell og tiltak blir testet.

Øvelser bør evalueres i alle ledd for å kunne identifisere hva som fungerer og ikke fungerer når det oppstår en hendelse og for å videreutvikle virksomhetens sikkerhet. Tester og øvelser med fysiske sikkerhetstiltak kan inkluderes i andre lignende øvelser som utføres i virksomheten som brannøvelse, mottak av trusler og evakueringsøvelser.

Øvelser bør inkludere involvering av en ekstern aktør som utfører sikkerhetstruende aktivitet. Hensikten er at virksomheten ikke er klar over detaljene og dermed får en mer reell opplevelse. Har virksomheten inngått avtaler med eksterne eller interne sikringsstyrker bør også disse inkluderes i øvelsen.

Hvorfor er dette viktig: Tester og øvelser er viktig for at virksomheter skal være sikre på at de fysiske sikkerhetstiltakene vil fungere som forventet ved en sikkerhetstruende hendelse og ikke utgjøre større skade.

Anbefalte tiltak:

- Utarbeid plan for gjennomføring av øvelser
- Inkluder eksterne samarbeidspartnere i utformingen av øvelser
- Test ansattes handlingsmønster ved hendelse
    - Evakuering
    - «Lock down»
- Kontroller at etablerte sikkerhetstiltak fungerer etter sin hensikt også ved utløst alarm
- Øv på sikring av verdier slik at disse ikke blir kompromittert ved utløst alarm

3. Opprettholde og oppdage

Formålet med denne kategorien er at virksomheten skal være i stand til å opprettholde den sikre tilstanden over tid og ved endringer samt skape forutsetning for å oppdage avvik. Prinsippene i denne kategorien ivaretar behovet for å håndtere både forutsette og uforutsette endringer. Sentralt her er å kontrollere at tiltakene fungerer etter sin hensikt, og oppdage avvik fra ønsket sikkerhetsnivå.

3.1. Vedlikeholde

Virksomheten bør sørge for at sikkerhetstiltak og tilhørende utstyr fungerer som det skal og blir jevnlig vedlikeholdt.

Virksomheten bør påse at det kun er autorisert personell som utfører vedlikehold og reparasjoner på utstyr og sikkerhetstiltak. Om det er nødvendig med større reparasjoner som vil ta lengre tid og sette sikkerhetstiltaket ut av funksjon i løpet av denne perioden, bør det opprettes midlertidige sikkerhetstiltak som fortsatt ivaretar beskyttelsen.

Hvorfor er dette viktig: Sikkerhetstiltakene bør vedlikeholdes slik at de varer lengre og ivaretar sikkerheten til virksomheten over tid, og dermed kan forhindre at feil og avvik oppstår uten at det blir oppdaget.

Anbefalte tiltak:

- Sørge for at sikkerhetstiltakene består over tid
- Etabler rutiner for jevnlig kontroll av etablerte sikkerhetstiltak
- Inngå avtaler med leverandører som kan drifte og vedlikeholde etablerte sikkerhetstiltak
- Planlegg for vedlikehold av tiltak, inkludert midlertidige tiltak for å ivareta ønsket sikkerhetsnivå
- Sørg for å gjennomføre kontroll etter reparasjoner og vedlikehold

3.2. Kontrollere de fysiske sikkerhetstiltakene

De fleste sikkerhetstiltak som er implementert bør kontrolleres jevnlig for å sikre at de fortsatt fungerer etter hensikt. Virksomheten bør sørge for at avvik ved sikkerhetstiltakene blir fanget opp, slik at nødvendig utbedring blir iverksatt. Avvik ved tiltakene kan være rondeller som ikke åpner seg når de skal, hull i gjerder som må tettes eller dører som ikke gir alarm når de blir åpnet. Sikkerhetstiltak som er etablert på utsiden av bygninger som kameraer, gjerder og pullerter bør sjekkes jevnlig da de er mer utsatt for ytre påvirkning, som dårlig vær og destruksjon.

Hvorfor er dette viktig: Ved jevnlig kontroll av fysiske sikkerhetstiltak vil virksomheten oppdage avvik og opprettholde ønsket sikkerhetsnivå over tid.

Anbefalte tiltak:

- Kontroller at de fysiske sikkerhetstiltakene fungerer som forventet
  - Rutinemessig kontroll
  - Øvelser / tester
  - Innmelding av avvik fra ansatte
  - Revisjon
- Sørg for rutine for registrering av avvik
- Kontroller og håndter avvik

3.3. Opprettholde gode endringsrutiner

Virksomheten bør sørge for at sikkerheten blir opprettholdt ved forutsette og uforutsette endringer. I utforming av risikovurdering bør det planlegges for ulike scenarioer som kan påvirke virksomheten. For å kunne håndtere endringer i trusselbildet bør virksomheten ha utformet planer med tilhørende tiltak som kan iverksettes ved behov. Ved en varig forhøyet trussel bør påbygningstiltak kunne innarbeides som en del av grunnsikringen og nye påbygningstiltak planlegges.

Hvorfor er dette viktig: Virksomheten bør opprettholde gode endringsrutiner for å være forberedt ved endringer og effektiv kunne håndtere økt risiko uten at det reduserer sikkerhetsnivå.

Anbefalte tiltak:

- Plan for grunnsikring, påbygningstiltak og skadebegrensende tiltak
- Sørg for at det er tilgjengelige påbygningstiltak
- Kommuniser planverk til personell med tjenstlig behov
- Sørge for helhetlig sikring også når påbygningstiltak er iverksatt
- Vurder om det er behov for at påbygningstiltak skal bli en del av grunnsikringen
  - Evakuering
  - Destruering
- Sørg for klar rollefordeling og kommuniser dette gjennom et tydelig planverk
- Involver tredjeparter som politi eller andre reaksjonsstyrker
- Sørg for at verdienes sikkerhet ivaretas under øvelser
- Evaluer øvelsen i alle ledd for å sikre lærdom og utvikling

4. Håndtere og gjenopprette

Hensikten med denne kategorien er å etablere rutiner for å effektivt kunne håndtere sikkerhetstruende virksomhet og avvik. Dette innebærer prinsipper for å vurdere, kontrollere og håndtere hendelser samt gjenopprette normaltilstand.

4.1. Håndtere hendelser

Virksomhetens håndtering av hendelser avhenger av hendelsens natur og alvorlighetsgrad. Ulike hendelser krever ulike reaksjoner og virksomheten bør identifisere hva slags type hendelse som pågår og hvilke tiltak som bør igangsettes. Ved å identifisere og vurdere uønskede hendelser som sikkerhetstruende virksomhet og avvik, vil virksomheten være i stand til å prioritere og distribuere ressursene der det er størst behov. Feilaktige vurderinger kan føre til at virksomheter bruker mye tid og krefter på mindre avvik.

Hvorfor er dette viktig: God hendelseshåndtering er viktig for å sikre at sikkerhetstruende virksomhet blir håndtert effektivt og korrekt.

Anbefalte tiltak:

- Sørg for rutiner, prosedyrer og beredskapsplaner
- Vurder pågående hendelser for å identifisere korrekte tiltak
- Sørg for proporsjonal respons på hendelsen
- Sørg for at ansatte er godt kjent med roller og oppgaver ved hendelser

4.2. Gjenopprette sikkerhetsnivå

For at virksomheten best mulig skal kunne gjenopprette sikkerhetsnivå etter en hendelse bør det planlegges og legge til rette for gjenopprettingstiltak. Virksomheten bør ha en plan med tiltak for hvordan de skal gjenopprette ønsket sikkerhetsnivå etter sikkerhetstruende hendelse.

Hvorfor er dette viktig: Effektive gjenopprettingstiltak vil sørge for at virksomheten kan gjenopprette akseptabelt sikkerhetsnivå samt redusere risiko for skade og tap av verdier og funksjoner.

Anbefalte tiltak:

- Plan for gjenoppretting av ønsket sikkerhetsnivå
- Sørg for redundans og mulighet for gjenopprettelse av verdier
- Inngå avtaler med eksterne tjenesteleverandører som kan drifte og gjenopprette sikkerhetstiltak

4.3. Evaluere hendelsen

Etter en hendelse bør virksomheten kartlegge hendelsesforløp og evaluere om egne sikkerhetstiltak fungerte etter sin hensikt. På bakgrunn av identifisere sårbarheter og avvik bør virksomheten kartlegge muligheter for implementering av andre, korrigerende fysiske sikkerhetstiltak. Virksomheten bør evaluere hendelsen og håndteringen for å lære, gjennomgå hendelsesprosesser, opplæring av personell og oppdatering av gjeldende tiltak.

Hvorfor er dette viktig: Hendelser bør evalueres slik at virksomheten og de involverte skal kunne ta lærdom av hendelsen og med dette forbedre sikkerheten.

Anbefalte tiltak:

- Etabler gode rutiner for evaluering og tilbakemelding etter hendelser
- Kartlegg styrker og sårbarheter i egen virksomhet
- Gjennomfør evaluering med andre involverte parter

4.4. Lær av erfaringer og implementer forbedringer

På bakgrunn av hendelseshåndtering og evaluering av hendelseshåndteringen bør virksomheten identifisere forbedringspunkter for å kunne heve sikkerheten til ønsket nivå. Virksomheten bør gjennomgå alle sine tiltak og identifisere hva som fungerte og ikke fungerte samt hvorfor. Hendelsen vil gi en indikasjon på om virksomhetens valg av fysiske sikkerhetstiltak oppnådde ønsket effekt mot identifisert trusselbilde. Funnene bør integreres i en oppdatert risikovurdering som igjen skaper forutsetninger for det videre sikkerhetsarbeidet.

Hvorfor er dette viktig: Basert på evalueringen av hendelseshåndteringen bør virksomheten implementere forbedringer slik at lignende hendelser kan håndteres effektiv og dermed opprettholde akseptabel sikkerhet.

Anbefalte tiltak:

- Innarbeid eventuelle endringer i planverket
- Implementer permanente korrigerende tiltak
- Evaluer om de korrigerende tiltakene fungerer som forutsatt
- Oppdater risikovurdering etter hendelse, avvik eller endring

Nasjonal sikkerhetsmyndighet

Postboks 814
1306 Sandvika

postmottak@nsm.no
www.nsm.no