Vagt i højsikkerhedsområder

SUS, Serviceerhvervenes
Efteruddannelsesudvalg

Udviklet af:
Rolf Ingemann Hartelius, UCplus
Thomas Kristian Skaarup, Aarhus Tech

December 2025

Vagt i højsikkerhedsområder

SUS

Serviceerhvervenes Efteruddannelsesudvalg
Vesterbrogade 6D, 4.

1620 København V.
Tlf. 32 54 50 55
www.susudd.dk
sus@sus-udd.dk

Indholdsfortegnelse

Indledning

Fra det øjeblik vi vågner om morgenen og tænder lyset, tjekker vores telefoner og begiver os på arbejde eller i skole, er vi dybt afhængige af kritisk infrastruktur. Disse fundamentale systemer holder samfundet kørende døgnet rundt. Det er netop i beskyttelsen af disse vitale funktioner, at vagter i højsikkerhedsområder spiller en afgørende og ofte underbelyst rolle.

Højsikkerhed dækker over områder og funktioner, hvor sikkerhedsbrud kan få alvorlige konsekvenser for samfundet som helhed. Det handler om meget mere end blot fysisk sikring. Som vagt i højsikkerhedsområder skal du besidde mental parathed, juridisk forståelse og evnen til at agere korrekt under pres. Du indgår i en større sikkerhedsstruktur, hvor dine handlinger kan have direkte indflydelse på samfundets stabilitet og sikkerhed. Højsikkerhedsområder kendetegnes ved, at de har stor symbolsk eller strategisk værdi, og selv mindre sikkerhedshændelser kan få vidtrækkende konsekvenser. Eksempler omfatter militære installationer, forsyningsanlæg som elværker og vandforsyning, transportknudepunkter som lufthavne og havne, datacentre med følsomme informationer, finansielle institutioner og kritiske sundhedsfaciliteter.

Det nuværende sikkerhedspolitiske klima har skabt et markant øget behov for professionel sikring af kritisk infrastruktur. Flere faktorer bidrager til denne udvikling. Internationale spændinger og hybride angreb fra fremmede stater udgør en stigende risiko, hvor både fysiske og digitale metoder anvendes til at destabilisere nationale strukturer. Samtidig oplever vi en markant stigning i cyberkriminalitet og cyberaktivisme, hvor både organiserede grupper og enkeltpersoner forsøger at kompromittere systemer og data. Truslen fra terrorisme og radikalisering forbliver aktuel, og organiseret kriminalitet samt industrispionage udgør en betydelig fare for både offentlige og private aktører. Den stigende digitalisering og den tætte sammenkobling mellem teknologiske systemer har gjort samfundet mere sårbart. Mange sektorer er afhængige af globaliserede forsyningskæder, hvilket øger risikoen for afbrydelser og manipulation.

Som højsikkerhedsvagt fungerer du som den første og ofte mest kritiske barriere mod alvorlige sikkerhedstrusler. Dine kernekompetencer omfatter avanceret adgangskontrol, hvor du kombinerer tekniske systemer med menneskelig intuition og trænet observation. Du skal kunne analysere adfærd og genkende tegn på nervøsitet, afvigende opførsel eller forsøg på manipulation gennem træning i mikroudtryk, kropssprog og stressindikatorer. Vedvarende sikkerhedsbevidsthed og mental parathed er kritisk, og du skal være opmærksom på hvordan både din egen og andres fysiske og digitale adfærd kan skabe udfordringer for sikkerheden. Professionel kommunikation og samarbejde med politi, beredskab og sikkerhedsansvarlige skal være klar, præcis og rettidig. Du er ofte det første led i en sikkerhedskæde, og kvaliteten af din rapportering kan være afgørende for den samlede respons. Endelig skal du kende og overholde reglerne for visitation, ransagning og anden myndighedsudøvelse samt forstå hvordan lovgivning og procedurer påvirker dit arbejde.

Højsikkerhed og kritisk infrastruktur

Højsikkerhedsområder adskiller sig fundamentalt fra almindelige sikkerhedsobjekter ved deres potentielle indvirkning på samfundet som helhed. Som Politiets Efterretningstjeneste definerer det, er disse områder karakteriseret ved at sikkerhedsbrud kan få alvorlige konsekvenser for samfundet på tre kritiske dimensioner. For det første menneskeligt tab med direkte fare for liv og sundhed. For det andet økonomiske konsekvenser der kan påvirke samfundet finansielt. For det tredje politiske følgevirkninger der kan destabilisere samfund og institutioner. Den strategiske værdi af højsikkerhedsområder ligger ofte i deres evne til at koncentrere store værdier på relativt begrænsede områder.

Kritisk infrastruktur i Danmark og Europa er defineret gennem den danske implementering af CER-loven, som trådte i kraft i maj 2025. Denne lov udgør Danmarks implementering af det europæiske CER-direktiv om kritiske enheders modstandsdygtighed. Loven fastlægger detaljerede krav til identifikation, beskyttelse og overvågning af kritiske enheder på tværs af elleve centrale sektorer. Disse omfatter energi, transport, bankvirksomhed, finansmarkedsinfrastruktur, sundhed, drikkevand, spildevand, digital infrastruktur, offentlig forvaltning, rummet samt produktion, forarbejdning og distribution af fødevarer.

Det aktuelle trusselsbillede mod Danmark er komplekst og mangefacetteret. Statslige aktører udgør den mest betydelige trussel mod kritisk infrastruktur. Som beskrevet i Forsvarets Efterretningstjenestes og Politiets Efterretningstjenestes årlige vurderinger står Danmark over for vedvarende trusler fra både cyberspionage og fysisk infiltration fra fremmede efterretningstjenester. Rusland vurderes at udgøre den mest alvorlige trussel mod dansk kritisk infrastruktur, med både kapacitet og intention til at udføre sabotageoperationer mod dansk infrastruktur som led i hybride påvirkningsoperationer. Kina udgør ligeledes en betydelig trussel, primært gennem cyberspionage og langsigtede påvirkningsoperationer. Iran og Nordkorea bidrager til trusselsbilledet gennem både cyberangreb og potentiel støtte til proxygruppers aktiviteter mod vestlige interesser. Cyberkriminalitet og ransomware udgør en konstant og stigende trussel mod kritiske systemer, hvor kriminelle organisationer målretter både offentlige og private infrastrukturaktører med sofistikerede angrebsmetoder.

Forskellige typer højsikkerhedskunder har varierende krav og forventninger, hvilket påvirker din rolle som vagt betydeligt. Offentlige myndigheder og statslige installationer opererer under strenge sikkerhedsklassifikationer og nationale sikkerhedsprotokoller. Her kan din rolle omfatte håndtering af klassificeret materiale, koordinering med efterretningstjenester og stringent adgangskontrol baseret på sikkerhedsgodkendelser. Private kritiske infrastrukturaktører fokuserer typisk på både fysisk sikkerhed og forretningskontinuitet. Forsyningsselskaber prioriterer opretholdelse af serviceleverance og beskyttelse mod både fysiske og digitale trusler. Finansielle institutioner balancerer kundeservice med omfattende sikkerhedskrav og skal beskytte både fysiske værdier og digitale transaktionssystemer. Internationale organisationer og ambassader har ofte særlige diplomatiske sikkerhedskrav og skal beskyttes mod både almindelig kriminalitet og statslig spionage.

Samfundskonsekvenser ved sikkerhedsbrud i kritisk infrastruktur kan være omfattende og langvarige. Umiddelbare konsekvenser omfatter direkte tab af menneskeliv eller sundhedsskader gennem angreb eller uheld i kritiske faciliteter, økonomiske tab fra afbrudte tjenester, ødelagt udstyr eller afpresning samt samfundsforstyrrelser hvor borgere mister adgang til basale tjenester som elektricitet, vand eller kommunikation. Operationelle konsekvenser inkluderer kaskadeeffekter hvor nedbrud i én sektor påvirker andre afhængige sektorer, og genoprettelsesomkostninger som kan være betydelige både økonomisk og tidsmæssigt. Strategiske og politiske konsekvenser kan omfatte tab af offentlig tillid til myndigheders evne til at beskytte samfundet, geopolitisk sårbarhed hvor Danmarks internationale position kan svækkes og sikkerhedspolitiske reaktioner med langsigtede ændringer i forsvar og sikkerhedspolitik.

Vagtens rolle og ansvar

Som højsikkerhedsvagt opererer du inden for et komplekst juridisk landskab, der definerer både dine rettigheder og forpligtelser. Det kontraktuelle grundlag for dit arbejde etableres gennem den aftale, som dit vagtfirma har indgået med kunden. Denne kontrakt specificerer dine opgaver, beføjelser og ansvarsområder, og du skal være fuldt fortrolig med dens indhold. Vagtvirksomhedsloven og tilhørende bekendtgørelser etablerer de overordnede juridiske rammer for dit arbejde og definerer hvilke opgaver vagtvirksomheder må udføre, krav til uddannelse og certificering samt tilsyns- og kontrolmekanismer. Straffeloven og Retsplejeloven fastlægger dine beføjelser og begrænsninger i forhold til magtanvendelse, anholdelse og videregivelse af information til myndigheder.

Operationelle forventninger til dig som højsikkerhedsvagt er omfattende og krævende. Din kunde forventer pålidelig tilstedeværelse og professionel adfærd til enhver tid, proaktiv sikkerhedsbevidsthed hvor du ikke blot reagerer på hændelser, men aktivt søger at identificere og forebygge trusler, korrekt dokumentation og rapportering af alle sikkerhedsrelevante observationer samt diskretion og fortrolighed omkring kundens forretning, sikkerhedsforanstaltninger og eventuelle hændelser. Dit vagtfirma forventer at du repræsenterer firmaet professionelt, følger etablerede procedurer og retningslinjer, kommunikerer effektivt med både ledelse og kollegaer samt vedligeholder og udvikler dine faglige kompetencer løbende.

Samarbejde med andre aktører er en central del af dit arbejde. Dit forhold til politiet er fundamentalt for effektiv højsikkerhedsbeskyttelse. Du skal kende procedurerne for hvornår og hvordan du skal kontakte politiet, forstå forskellen mellem din rolle som privatansat sikkerhedsperson og politiets myndighedsrolle samt kunne kommunikere klart og præcist om sikkerhedshændelser. I nødsituationer er du ofte den første til at observere og reagere, men politiet har det overordnede kommandoansvar når de ankommer. Beredskabstjenester som brandvæsen og ambulancetjeneste skal du samarbejde tæt med, og du skal kende faciliteten indgående og kunne guide redningspersonale effektivt. Andre sikkerhedsaktører kan omfatte kundens interne sikkerhedsafdeling, andre vagtfirmaer der arbejder på samme eller tilstødende områder samt specialiserede sikkerhedskonsulenter eller tekniske leverandører.

Professionel kommunikation og rapportering er afgørende for effektivt sikkerhedsarbejde. Mundtlig kommunikation skal være klar, præcis og tilpasset modtageren. Når du kommunikerer med ledelse, skal du kunne præsentere information struktureret og handlingsorienteret. Med kollegaer skal kommunikationen være effektiv og understøtte teamwork. Overfor publikum eller besøgende skal du kunne forklare sikkerhedsprocedurer på en måde der er både informativ og betryggende uden at afsløre sensitive sikkerhedsdetaljer. Skriftlig rapportering udgør et kritisk juridisk og operationelt værktøj. Dine rapporter kan få stor betydning for efterfølgende undersøgelser eller retssager og skal derfor være objektive, detaljerede, velstrukturerede og rettidig udført.

Etik, diskretion og fortrolighed er fundamentale principper i højsikkerhedsarbejde. Professionel etik betyder at du skal behandle alle personer med respekt og værdighed uanset deres baggrund, anvende magt kun når det er nødvendigt og proportionalt, beskytte privatlivets fred samtidig med at sikkerhedskrav opretholdes samt være ærlig og transparent i din rapportering. Fortrolighed omfatter beskyttelse af kundens forretningshemmeligheder og sikkerhedsforanstaltninger, korrekt håndtering af persondata i overensstemmelse med databeskyttelsesforordningen samt diskretion omkring hændelser og personer du møder i dit arbejde. Håndtering af klassificeret information kræver særlig omhu hvor du skal kende klassifikationsniveauer og håndteringsregler, beskytte information mod uautoriseret adgang samt rapportere enhver mistanke om sikkerhedsbrud øjeblikkeligt.

Integration i den større sikkerhedsstruktur betyder at du ikke arbejder isoleret men som del af et komplekst sikkerhedsøkosystem. Dit bidrag til den nationale sikkerhedsarkitektur kan synes beskedent i dagligdagen, men den kumulative effekt af professionelt højsikkerhedsarbejde på tværs af kritisk infrastruktur er betydelig for Danmarks samlede modstandsdygtighed. Ved at udføre dit arbejde med høj standard bidrager du direkte til beskyttelse af samfundskritiske funktioner, afskrækkelse af potentielle trusselaktører samt styrkelse af offentlig tillid til sikkerhedssystemer.

Situationsbevidsthed og mental parathed

Situationsbevidsthed repræsenterer langt mere end blot at være opmærksom på sine omgivelser. Som defineret i den klassiske model omfatter det tre distinkte kognitive niveauer. For det første erkendelse af elementer i miljøet gennem aktiv indsamling af sensorisk information. For det andet forståelse af deres betydning gennem sammenligning med eksisterende viden og erfaring. For det tredje forudsigelse af deres fremtidige tilstand ved at anvende information fra de første to niveauer til at foregribe sandsynlige fremtidige udviklinger. Denne tredimensionelle tilgang til bevidsthed skaber grundlaget for effektivt sikkerhedsarbejde i højsikkerhedsområder, hvor evnen til at forstå komplekse situationer og forudse udviklingen kan være afgørende for både personlig sikkerhed og beskyttelse af kritiske ressourcer.

Menneskelig opfattelse og informationsbehandling er behæftet med systematiske fejl og begrænsninger, der kan kompromittere situationsbevidsthed. Bekræftelsesbias fører til at vi søger information der bekræfter eksisterende antagelser, mens vi ignorerer eller nedvurderer

modstridende beviser. Normalitetsbias får os til at undervurdere sandsynligheden eller alvoren af sjældne men alvorlige begivenheder som terrorangreb eller naturkatastrofer. Tunnelsyn betyder at vi kan overse selv tydelige stimuli, hvis vores opmærksomhed er fokuseret andre steder. Forståelse af disse kognitive begrænsninger er det første skridt mod at udvikle modstrategier.

Cooper's Color Code system, udviklet i halvfjerdserne til militær og politimæssig anvendelse, tilbyder en systematisk tilgang til mental beredskab og taktisk bevidsthed. Systemet blev designet som en mental model til at standardisere kommunikation omkring beredskabsniveauer og sikre passende reaktioner på varierende niveauer af opfattede trusler. Niveau Hvid repræsenterer manglende situationsbevidsthed og maksimal sårbarhed over for overraskelsesangreb. Personer i denne tilstand er opslugte af andre aktiviteter og udviser ingen opmærksomhed på deres miljø eller potentielle trusler. Niveau Gul udgør det optimale operationelle beredskabsniveau for højsikkerhedsvagter under normale forhold. Du er bevidst om dine omgivelser, scanner aktivt for potentielle trusler og er mentalt forberedt på at reagere hvis nødvendigt. Niveau Orange aktiveres når du identificerer en specifik potentiel trussel, og din mentale fokus skærpes betydeligt. Niveau Rød indtræffer når en direkte trussel manifesterer sig og kræver øjeblikkelig handling, hvor din træning og forberedelse omsættes til kontrolleret og effektiv respons.

OOBH-metoden tilbyder en struktureret tilgang til beslutningstagning under tidspres. Observere fasen involverer systematisk indsamling af information om situationen gennem alle tilgængelige kanaler. Overveje fasen analyserer den indsamlede information, identificerer mulige handlemuligheder og vurderer deres sandsynlige konsekvenser. Beslutte fasen vælger den mest hensigtsmæssige handling baseret på analysen, hvor beslutningen skal være informeret af både rationel vurdering og professionel træning. Handle-fasen implementerer den valgte handling med fuldt engagement, og effektiv udførelse kræver at du har tillid til din beslutningsproces og kan handle resolut trods usikkerhed.

Mental parathed under stresshåndtering kræver både fysiologisk og psykologisk forberedelse. Fysiologiske stressresponsmekanismer aktiveres automatisk under truende situationer og omfatter øget hjertefrekvens og blodtryk, udskillelse af adrenalin og kortisol, skærpede sanser og reduceret smerteølsomhed samt omdirigering af blod fra fordøjelsessystemet til muskler. Kontrolleret vejrtrækning er en af de mest effektive teknikker til at modulere stressrespons, hvor dybe, langsomme åndedrag aktiverer parasympatisk nervesystem og modvirker kampflugt responsen. Progressiv muskelafslapning involverer systematisk spænding og afslapning af muskelgrupper gennem kroppen og reducerer fysisk spænding og fremmer mental klarhed. Visualiseringsteknikker forbereder dig mentalt på potentielle situationer gennem regelmæssig mental gennemgang af procedurer og scenarier.

Kontinuerlig træning og udvikling af bevidsthed kræver systematisk praksis og engagement i vedvarende forbedring. Daglige bevidsthedsøvelser kan inkorporeres i rutineaktiviteter og hjælper med at opbygge fundamentale observationskapaciteter. Simple øvelser som farvet bil spillet, hvor du vælger en farve og tæller alle biler af den farve du ser i løbet af dagen, udvikler systematisk miljøscanning. Hukommelsesøvelser hjælper med at udvikle kapacitet til at bevare

og analysere observationsinformation, hvor du øver dig i at memorere detaljer om mennesker du møder og derefter teste din genkaldelsesnøjagtighed senere. Forudsigelsesøvelser hjælper med at

udvikle situationsbevidstheden ved at kræve at du foregriber fremtidige begivenheder baseret på nuværende observationer.

Observation og adfærdsanalyse

Systematisk observation er fundamentet for effektivt sikkerhedsarbejde i højrisikoområder. Som sikkerhedsprofessionel skal du kunne skelne mellem et normalt adfærdsmønster og afvigende adfærd som kunne indikere potentielle sikkerhedstrusler. Din observationsevne skal være struktureret, konsekvent og baseret på objektive indikatorer snarere end subjektive indtryk. Normalbilledet for dit specifikke område er dit primære referencepunkt. Som betonet i de foregående kapitler, er vagtens fortrolighed med de lokale omgivelser en fordel, der gør vagten til ekspert i nærmiljøet. Dette lokale kendskab tillader dig at identificere selv subtile afvigelser fra det normale aktivitetsmønster.

Etablering af et pålideligt grundniveau kræver kontinuerlig observation af normale adfærdsmønstre under forskellige betingelser. Du skal dokumentere systematisk normale trafikmønstre for at forstå hvornår folk kommer og går og hvilke ruter de normalt bruger. Du skal observere befolkningssammensætning for at forstå hvilke typer personer der normalt er til stede på forskellige tidspunkter. Du skal lære adfærdsnormer for at forstå hvordan folk normalt opfører sig i forskellige områder af faciliteten. Særlig opmærksomhed skal gives til personer der kommer flere gange på samme lokalitet, udviser særlig interesse i højrisikoområder, virker nervøse, tager billeder af bevogtningsområdet eller forsøger at gemme sig når de ser vagten. Spørg dig selv om en persons adfærd er naturlig på dette tidspunkt i disse omgivelser og i forhold til normalbilledet.

Kropssprog og nonverbal kommunikation bidrager i langt højere grad til forståelsen af et budskab eller en samtale end det der bliver sagt, og dette sker helt ubevidst. Som sikkerhedsvagt skal du kunne aflæse både andre menneskers nonverbale signaler og være bevidst om dine egne. Ansigt og hoved giver værdifulde indikatorer for stress og vildledning. Minimal øjenkontakt eller overdreven øjenkontakt kan indikere ubehag eller forsøg på manipulation. Hurtige blik mod udgange eller flugtruter kan signalere flugtforberedelse. Anspændte kæbemuskler eller sammenbidte tænder indikerer stress, mens et overdrevet smil eller unaturligt ansigtsudtryk kan være forsøg på at skjule ægte følelser. Kropsholdning og bevægelser afslører ligeledes vigtige informationer. Stiv eller unaturlig kropsholdning kan indikere nervøsitet eller skjulte motiver. Urolige bevægelser, fingerering eller rastløshed signalerer ofte indre stress eller usikkerhed.

Mikroudtryk er ufrivillige korte ansigtsudtryk som varer normalt brøkdel af et sekund og afslører autentiske følelser som personer forsøger at skjule. Den banebrydende forskning har udviklet videnskabsbaserede træningsværktøjer til genkendelse af skjulte følelser gennem ansigtsudtryk. De syv universelle følelser som er identificeret viser sig på samme måde på tværs af kulturer. Disse omfatter glæde med løftede mundvige og rynker omkring øjnene, overraskelse med hævede øjenbryn og åben mund, frygt med vidtåbne øjne og spændt ansigt, vrede med rynkede

øjenbryn og sammenknebne øjne, afsky med rynket næse og løftet overlæbe, tristhed med sænkede mundvige og sænkede øjenbryn samt foragt med ensidigt løftet mundvig.

Adfærdsmæssig trusselsvurdering kræver systematisk anvendelse af dokumenterede metoder. Systematisk observation af afvigende adfærd danner grundlag for professionel trusselsvurdering. Du skal være opmærksom på usædvanlig interesse i sikkerhedsforanstaltninger, overdreven nervøsitet eller unormal adfærd i forhold til konteksten, uoverensstemmelser mellem påstået formål og faktisk adfærd samt forsøg på at undgå observation eller kameraer. Baseline sammenligning indebærer at du sammenligner observeret adfærd med det etablerede grundniveau for området, konteksten og den specifikke situation. En persons adfærd kan være helt normal i én kontekst men højst mistænkelig i en anden.

Kulturelle og kontekstuelle faktorer i adfærdstolkning skal altid overvejes for at undgå uretfærdig profilering og sikre objektiv sikkerhedsvurdering. Kulturel baggrund påvirker betydeligt nonverbal kommunikation. Normer for øjenkontakt varierer betydeligt mellem kulturer, hvor det der virker mistænkeligt i én kultur, kan være normalt høflighedsadfærd i en anden. Gestikulation og berøring har forskellige normer på tværs af kulturer for acceptable gestikulation og fysisk kontakt. Størrelsen på personlige sfære varierer markant mellem kulturer, og det der opleves som passende afstand i én kultur kan virke invasivt eller afvisende i en anden. Udvikling af kulturel følsomhed sikrer objektiv analyse uden at lade fordomme påvirke din vurdering.

Overvågning af lokalområdet

Systematisk rundering er langt mere end blot at gå rundt i et område. Det kræver en struktureret tilgang der sikrer omfattende dækning af alle sikkerhedskritiske områder mens du opretholder en upåklagelig og variabel timing der forhindrer potentielle trusler i at forudsige dine bevægelser. Effektiv patruljering baserer sig på grundige forhåndskendskab til området. Du skal kende hver bygning, hver indgang, alle sikkerhedssystemer og potentielle sårbarheder. Dette kendskab opbygges gennem systematisk kortlægning af faciliteten, hvor du identificerer kritiske kontrolpunkter, potentielle infiltrationsruter, flugtveje og områder med begrænset synlighed eller adgang.

Runderingsbeskrivelsen angiver en rute gennem virksomheden med en række kontrolpunkter som vagten skal passere i en bestemt rækkefølge, og disse punkter skal aflæses med elektroniske kontrolsystemer der dokumenterer din tilstedeværelse og tidspunkt. Variabel patruljering er afgørende for at forhindre at potentielle trusler kan forudsige dine bevægelser og udnytte dette til at omgå sikkerhed. Du skal variere tidspunkter for dine runderinger inden for acceptable rammer, anvende forskellige ruter mellem kontrolpunkter når muligt samt ændre rækkefølgen af ikke kritiske kontrolpunkter. Fokuserede observationer under patruljering kræver at du har specifikke observationspunkter for hver del af ruten. Ved hver kritisk lokation skal du udføre systematisk scanning af området, kontrollere integriteten af fysiske sikkerhedsforanstaltninger, verificere at adgangskontrolsystemer fungerer korrekt samt notere enhver afvigelse fra det normale.

Brug af overvågningsudstyr og teknologi udvider betydeligt din observationskapacitet og giver mulighed for kontinuerlig overvågning af områder som ville være umulige at dække alene gennem fysisk tilstedeværelse. Videoovervågningssystemer udgør kernen i moderne sikkerhedsteknologi for højsikkerhedsområder. Analoge systemer anvender traditionelle kameraer og videobånd eller digitale optagelsesenheder. Selvom disse systemer gradvist fases ud, findes de stadig i mange ældre installationer. IP baserede systemer transmitterer video over computernetværk og tilbyder betydeligt højere opløsning, fleksibilitet og integrationsmuligheder. Moderne IP-kameraer kan inkludere avancerede funktioner som bevægelsesdetektion, ansigtsgen kendelse og automatiske alarmer ved specifikke hændelser.

Registrering og dokumentation af observationer er et fundamentalt ansvar der har både operationel og juridisk betydning. Dine observationer og notater kan blive afgørende bevismateriale i efterfølgende undersøgelser eller retssager, så præcision og objektivitet er absolut essentielle. Logbogsføring udgør den primære metode for løbende dokumentation af din vagt. Enhver logbog skal indeholde grundlæggende information om vagtens start og sluttidspunkt, vejrforhold og andre miljøfaktorer samt navne på vagter på tjeneste. Løbende notater skal dokumentere tidspunkt for hver rundering og kontrolpunkt besøg, alle observationer af afvigelser fra det normale, interaktioner med personer på området samt tekniske problemer eller systemfejl.

Identifikation af afvigelser og mistænkelig adfærd kræver både systematisk observation og intuitiv forståelse af hvad der udgør normal versus unormal aktivitet i dit specifikke miljø. Som beskrevet i kapitel fem om adfærdsanalyse, er etablering af et solidt grundniveau for normal aktivitet fundamentet for at kunne identificere meningsfulde afvigelser. Fysiske afvigelser i miljøet kan

manifestere sig på mange måder. Du skal være opmærksom på åbne døre eller vinduer der normalt er lukkede, beskadigede låse eller sikkerhedsforanstaltninger, uautoriserede køretøjer på området samt efterladte genstande eller pakker. Tidsmæssige afvigelser involverer aktiviteter der finder sted på usædvanlige tidspunkter. Vær særligt opmærksom på personer til stede uden for normale arbejdstider, leverancer eller servicebesøg der ikke er planlagt, usædvanlig trafik eller bevægelse om natten samt aktivitet i områder der normalt er ubeboede på bestemte tidspunkter.

Miljøbevidsthed og CPTED-principper integrerer fysisk design med sikkerhedsstrategi for at skabe miljøer der naturligt modvirker kriminalitet og uautoriseret aktivitet. CPTED står for Crime Prevention Through Environmental Design og repræsenterer en holistisk tilgang til sikkerhed der går ud over traditionelle låse og alarmer. Naturlig overvågning maksimerer synlighed og observationsmuligheder gennem strategisk placering af vinduer, belysning og landskab. Områder med høj naturlig overvågning oplever betydeligt mindre kriminalitet fordi potentielle gerningsmænd ved at de let kan blive observeret. Adgangskontrol gennem miljødesign styrer bevægelser gennem rummet ved at skabe klare distinktioner mellem offentlige, halvoffentlige og private områder. Territorial forstærkning skaber psykologisk ejerskab til rum gennem design der kommunikerer at området er beskyttet og overvåget.

Lovgivning og retningslinjer

Dansk lovgivning etablerer de grundlæggende juridiske rammer for dit arbejde som højsikkerhedsvagt. Vagtvirksomhedsloven regulerer den kommercielle vagtvirksomhed og definerer hvilke opgaver vagtfirmaer må udføre, krav til uddannelse og certificering samt tilsyns- og kontrolmekanismer. Loven fastlægger at vagtvirksomhed kræver godkendelse fra politiet, og at vagter skal gennemføre godkendt uddannelse før de må arbejde. Retsplejeloven indeholder bestemmelser om private personers beføjelser til anholdelse og magtanvendelse. Som privatperson har du ret til at anholde personer du træffer i færd med at begå en lovovertrædelse som er underlagt offentlig påtale hvis visse betingelser er opfyldt, men din beføjelse er betydeligt mere begrænset end politiets. Straffeloven definerer hvilke handlinger der er strafbare og fastlægger straframmer. Som vagt skal du være særligt opmærksom på bestemmelser omkring vold, trusler, tyveri, hærværk og uautoriseret adgang.

CER-loven og EU-direktiver for kritisk infrastruktur etablerer specifikke krav til beskyttelse af samfundskritiske funktioner. Loven om kritiske enheders modstandsdygtighed trådte i kraft i Danmark i maj 2025 og implementerer det europæiske CER-direktiv. Loven identificerer kritiske enheder på tværs af elleve sektorer baseret på deres betydning for samfundets funktioner. Kritiske enheder er underlagt skærpede krav til risikovurdering og sikkerhedsforanstaltninger, rapportering af sikkerhedshændelser til relevante myndigheder samt regelmæssig evaluering og opdatering af sikkerhedsforanstaltninger. Som højsikkerhedsvagt ved faciliteter omfattet af CER-loven skal du forstå de specifikke forpligtelser dette medfører for både din kunde og dit vagtfirma.

Kundespecifikke sikkerhedsprocedurer udgør de detaljerede operationelle retningslinjer for dit daglige arbejde. Hver kunde i højsikkerhedssektoren har udviklet specifikke procedurer tilpasset deres unikke risikoprofil, operationelle krav og regulatoriske forpligtelser. Din forholdsordre udgør det primære dokument der definerer dine specifikke opgaver og ansvar. Dette dokument skal indeholde detaljeret beskrivelse af facilitetens layout og kritiske områder, runderingsruter og kontrolpunkter med specifikke observationskrav, procedurer for adgangskontrol og verifikation, kommunikationsprocedurer og kontaktinformation samt eskalationsprocedurer for forskellige typer hændelser. Forholdsordren fastlægger procedurerne for hvordan du skal håndtere afvigelser, nødsituationer og hvornår du skal eskalere sager til højere myndigheder.

Persondata og databeskyttelsesforordningen i sikkerhedsarbejde regulerer hvordan du må indsamle, behandle og opbevare personoplysninger. Som højsikkerhedsvagt håndterer du jævnligt personoplysninger gennem legitimationskontrol, adgangslogger, observationsrapporter og sikkerhedsdokumentation. Databeskyttelsesforordningen også kendt som GDPR fastlægger strenge krav til hvordan sådanne data skal behandles. Grundlæggende principper omfatter lovlighed, rimelighed og gennemsigtighed hvor databehandling skal have et lovligt grundlag og personer skal informeres om hvordan deres data bruges. Formålsbegrænsning betyder at data kun må indsamles til specifikke legitime formål og ikke senere bruges til andre formål. Dataminimering kræver at du kun indsamler data der er nødvendige for det angivne formål.

Myndighedsudøvelse og retssikkerhed definerer grænserne for hvad du må og ikke må gøre som privatansat sikkerhedsperson. Din myndighed som privatperson er fundamentalt begrænset

sammenlignet med politiets. Du har ikke særlige beføjelser ud over hvad almindelige borgere har medmindre specifikke lovbestemmelser eller kontraktuelle aftaler giver dig dette. Magtanvendelse må kun ske når det er absolut nødvendigt og skal altid være proportionalt med situationen. Unødvendig eller overdreven magt kan resultere i strafferetlige konsekvenser for dig personligt. Anholdelsesbeføjelse som privatperson er begrænset til situationer hvor du træffer en person i færd med at begå en lovovertrædelse som er underlagt offentlig påtale og hvor øjeblikkelig indgriben er påkrævet for at sikre gerningsmanden eller bevismateriale.

Visitation og ransagning

Juridiske rammer og begrænsninger for visitation og ransagning er komplekse og kræver omhyggelig forståelse for at sikre at dine handlinger er lovlige og forsvarlige. Som privatansat sikkerhedsperson har du ikke automatisk ret til at visitere eller ransage personer. Din beføjelse i denne henseende afhænger primært af eksplicit samtykke fra den person der skal visiteres eller klart kontraktlig hjemmel hvor personen ved at bede om adgang til området accepterer at undergå sikkerhedskontrol. Samtykke skal være informeret, frivilligt og specifikt. Personen skal forstå hvad visitationen involverer og have en reel mulighed for at nægte uden uretmæssigt pres eller konsekvenser ud over nægtelse af adgang.

Forskellen på visitation og ransagning er vigtig både juridisk og praktisk. Visitation refererer primært til undersøgelse af personers tøj og umiddelbart tilgængelige ejendele for at identificere skjulte genstande der kunne udgøre en sikkerhedsrisiko. Dette omfatter typisk scanning eller ydre fysisk undersøgelse af tøj, lommer og håndbagage uden at kræve afklædning eller intimere berøring. Ransagning er en mere omfattende undersøgelse af persons ejendele, køretøjer eller andre private områder hvor personen har en rimelig forventning om privatliv. Ransagning kræver stærkere juridisk hjemmel end visitation og involverer typisk systematisk gennemsøgning af indhold i tøj, tasker, køretøjer eller andre private rum.

Procedurer og protokoller for visitation og ransagning skal følges nøje for at sikre både effektivitet og respekt for personers rettigheder. Forberedelse og kommunikation før enhver visitation er afgørende. Du skal verificere at du har juridisk grundlag for visitationen enten gennem samtykke, kontraktuel hjemmel eller kundespecifikke procedurer. Du skal informere personen klart om hvad proceduren involverer og hvorfor den er nødvendig. Du skal indhente eksplicit samtykke hvor dette er påkrævet og dokumentere dette samtykke. Ved manuel visitation skal du så vidt muligt anvende visitator af samme køn som den person der visiteres og sikre at visitationen foregår i et privat område hvor personen ikke udsættes for unødig offentlig ydmygelse.

Dokumentation og rapportering af visitationer og ransagninger er afgørende både for operationel effektivitet og juridisk beskyttelse. Hver visitation skal dokumenteres med tidspunkt og sted for visitationen, navn på den person der blev visiteret hvis kendt, navn på den eller de vagter der udførte visitationen, grundlag for visitationen samt resultat af visitationen. Ved fund af forbudte genstande skal du detaljeret beskrive hvad der blev fundet, fotografere genstandene hvis muligt og relevant samt følge etablerede procedurer for håndtering og overdragelse til myndigheder.

Håndtering af konflikter og klager i forbindelse med visitation kræver både professionalisme og forståelse for at visitationer kan opleves som invasive og ubehagelige selv når de udføres korrekt. Forebyggelse af konflikter starter med klar kommunikation før visitationen. Forklar tydeligt hvorfor visitationen er nødvendig, hvad den involverer og hvordan den udføres. Vær høflig og respektfuld i din tone og adfærd. Giv personen mulighed for at stille spørgsmål og adresser bekymringer. Ved modstand eller nægtelse skal du først forsøge at forstå personens bekymringer og adressere dem hvis muligt. Hvis personen fortsætter med at nægte og samtykke er påkrævet kan du ikke gennemtvinge visitationen men må i stedet nægte adgang til området.

Adgangskontrol i praksis

Identifikation og verificering udgør fundamentet for effektiv adgangskontrol. Som højsikkerhedsvagt er din primære opgave at sikre at kun autoriserede personer får adgang til beskyttede områder, og dette kræver omhyggelig verificering af identitet og adgangsrettigheder. Primær identifikation involverer validering af officiel foto legitimation som pas, kørekort eller nationalt identitetskort. Du skal verificere at billedet matcher personen, kontrollere at dokumentet ikke er tydeligt forfalsket, verificere at dokumentet ikke er udløbet samt notere relevante detaljer som navn og dokumentnummer hvis påkrævet. Sekundær identifikation gennem adgangskort eller badges udstedt af organisationen giver både identificering og autorisation. Moderne adgangskort indeholder typisk foto, navn og ansættelsesdetaljer, magnetstribe eller RFID-chip med elektronisk autorisation, synlige sikkerhedsfeatures som hologrammer samt eventuelt biometriske data.

Teknologisk infrastruktur og integration har revolutioneret adgangskontrol i højsikkerhedsområder gennem integration af multiple verifikationsmetoder og automatisering af mange processer. Moderne adgangskontrolsystemer kombinerer forskellige teknologier for at opnå både høj sikkerhed og operationel effektivitet. Kortbaserede systemer anvender magnetkort eller RFID-teknologi til at identificere og autorisere personer. Disse systemer kan spore hvem der er hvor i faciliteten til enhver tid, kontrollere adgang baseret på tid og lokation samt generere detaljerede adgangslogger til sikkerhedsanalyse. Biometriske systemer tilføjer et ekstra sikkerhedslag ved at verificere unikke fysiske karakteristika. Fingeraftryk scanning er den mest almindelige biometriske metode på grund af balance mellem sikkerhed, omkostning og brugeraccept. Ansigtsgenkendelse bliver stadig mere sofistikeret og kan i nogle systemer fungere kontaktløst. Iris scanning tilbyder meget høj sikkerhed men er typisk reserveret til de mest følsomme områder på grund af højere omkostninger.

Operationelle procedurer og workflows for adgangskontrol skal balancere sikkerhed med effektivitet og kundeservice. Forskellige typer besøgende kræver forskellige verifikationsniveauer og procedurer. Forhåndsregistrerede besøgende har typisk lettere adgangsproces da deres besøg er planlagt og verificeret på forhånd. Du skal verificere identitet mod besøgsreservationen, udstede besøgsbadge og registrere ankomsttidspunkt samt informere værtsperson om besøgendes ankomst. Uanmeldte besøgende kræver mere omfattende verificering. Du skal verificere identitet grundigt, kontakte den person de ønsker at besøge for godkendelse samt afvente bekræftelse før adgang gives.

Avancerede sikkerhedsforanstaltninger implementeres i højsikkerhedsområder hvor trusselsniveauet er særligt højt eller hvor beskyttelsen af kritisk infrastruktur kræver ekstraordinære foranstaltninger. Manuelt tilsyn ledsaget adgang eller eskort kræver at besøgende til enhver tid ledsages af autoriseret personale. Dette anvendes i særligt følsomme områder hvor selv autoriseret adgang ikke er tilstrækkelig garanti alene. To faktor autentifikation kombinerer noget du har som et adgangskort med noget du ved som en pinkode eller noget du er som et biometrisk kendetegn. Dette reducerer betydeligt risikoen for uautoriseret adgang gennem stjålne eller tabte kort. Tidsbegrænsede adgangstilladelser sikrer at besøgskort og midlertidige autorisationer automatisk udløber efter en fastsat periode.

Håndtering af udfordringer og fejlsituationer i adgangskontrol kræver både teknisk kompetence og god dømmekraft. Systemfejl kan opstå på selv de mest pålidelige systemer, og du skal være forberedt på at håndtere disse situationer uden at kompromittere sikkerheden. Ved tekniske problemer med adgangskontrolsystemer skal du skifte til manuelle procedurer hvor du verificerer identitet gennem foto legitimation, kontakter autoriseret personale for bekræftelse, dokumenterer alle adgange manuelt samt rapporterer systemfejl øjeblikkeligt til teknisk support. Tabte eller stjålne adgangskort udgør en betydelig sikkerhedsrisiko da de potentielt kan bruges af uautoriserede personer. Ved rapportering af tabt eller stjålet kort skal du øjeblikkeligt deaktivere kortet i systemet, udstede midlertidigt erstatningskort med skærpet verifikation samt dokumentere hændelsen grundigt.

Integration med overordnet sikkerhedsstrategi betyder at adgangskontrol ikke fungerer isoleret men som en integreret komponent i et omfattende sikkerhedsøkosystem. Din rolle i adgangskontrol bidrager direkte til flere lag af organisationens sikkerhed. Perimeterbeskyttelse etablerer den første barriere mod uautoriseret adgang hvor du kontrollerer hvem der krydser grænsen mellem offentligt og privat område. Zoneopdeling inden for faciliteter kræver forskellige adgangsniveauer for forskellige områder baseret på følsomhed og risiko. Du skal sikre at personer kun får adgang til de zoner de er autoriseret til. Trusselsdetektion gennem observation af adfærd under adgangskontrolprocessen giver tidlig advarsel om potentielle sikkerhedstrusler.

Konflikthåndtering og kommunikation

Deeskalationsteknikker er fundamentale færdigheder for enhver højsikkerhedsvagt da konflikter er uundgåelige når du håndhæver regler og nægter adgang. Effektiv deeskalering kan forhindre at situationer udvikler sig til fysiske konfrontationer og beskytter både dig selv og andre. Konfliktens grundlæggende natur i sikkerhedsarbejdet adskiller sig fra hverdagskonflikter ved at involvere asymmetriske magtforhold, høje stressniveauer og potentielt alvorlige konsekvenser. Du repræsenterer autoritet og kontrol, hvilket automatisk påvirker dynamikken i enhver interaktion. Den første og vigtigste deeskaleringsteknik er at forblive rolig uanset provokation. Din kropslige ro, stemmeføring og ansigtsudtryk sætter tonen for hele interaktionen.

Verbal judo og påvirkningspsykologi giver dig værktøjer til at påvirke situationer og personer gennem strategisk kommunikation frem for fysisk magt. Begrebet verbal judo refererer til brugen af ord og kommunikationsteknikker til at deeskalere konflikter og opnå samarbejde på samme

måde som fysisk judo bruger modstanderens kraft mod dem selv. Empatisk anerkendelse af personens følelser og perspektiv er første skridt i verbal judo. Folk vil ofte deeskalere når de føler sig hørt og forstået selv om du ikke kan give dem hvad de ønsker. Du kan sige jeg kan se at dette er frustrerende for dig eller jeg forstår at du er i en pressende situation. Genindramning af situationen præsenterer samme information på en måde der gør det lettere for personen at acceptere. I stedet for du kan ikke komme ind kan du sige jeg vil gerne hjælpe dig med at få adgang når vi har fået verificeret din identitet.

Håndtering af nægtelse og modstand er en regelmæssig del af arbejdet i adgangskontrol hvor du må nægte adgang eller fjerne privilegier fra personer der kan være frustrerede eller vrede. Klar kommunikation af beslutningen skal ske roligt og bestemt. Du skal forklare hvad beslutningen er uden undskyldninger, angive den objektive grund til beslutningen, undgå at personalisere beslutningen samt tilbyde alternativer hvor det er muligt. Ved eskalerende modstand hvor personen bliver mere aggressiv eller truende skal du opretholde sikker afstand og give dig selv manøvrerum, aktivere din kommunikationsenhed og anmode om backup samt være forberedt på at personen kan blive fysisk.

Professionel kommunikation under pres kræver at du kan opretholde klarhed og effektivitet selv når situationer er stressende eller kaotiske. Dine kommunikationsevner under pres kan være forskellen mellem en vellykket løsning og en eskaleret krise. Stressens indvirkning på kommunikation manifesterer sig på flere måder. Kognitiv indsnævring reducerer din evne til at behandle kompleks information og kan føre til sort hvid tænkning. Emotionel reaktivitet gør det sværere at kontrollere dine egne følelser og kan føre til defensive eller aggressive reaktioner. Fysiologiske ændringer som hurtigere tale, højere stemme og spændte muskler kan forværre situationen. Bevidsthed om disse effekter er første skridt til at modvirke dem.

Kulturel forståelse og mangfoldighed er essentiel i moderne højsikkerhedsarbejde hvor du vil møde mennesker fra mange forskellige kulturelle baggrunde. Manglende kulturel sensitivitet kan skabe konflikter hvor ingen var nødvendig og kan føre til diskrimination der både er uetisk og potentielt ulovlig. Kulturelle forskelle i kommunikationsstil påvirker hvordan mennesker interagerer med autoritet. Direkte versus indirekte kommunikation varierer betydeligt hvor nogle kulturer

værdsætter direkte klar kommunikation mens andre foretrækker mere indirekte tilgange der bevarer ansigt. Hierarkisk orientering betyder at nogle kulturer har dyb respekt for autoritetsfigurer og vil typisk efterkomme instruktioner uden diskussion mens andre kulturer har mere egalitære holdninger og forventer at kunne diskutere eller udfordre autoriteter.

Krise og beredskabshåndtering

Aktiv risikovurdering og tidlige tegn på potentielle kriser er fundamentale kompetencer for højsikkerhedsvagter. Din evne til at identificere og respondere på tidlige advarselssignaler kan være forskellen mellem forebyggelse og katastrofe. Proaktiv trusselidentifikation kræver kontinuerlig opmærksomhed på indikatorer der kan signalere udvikling af sikkerhedstrusler. Adfærdsmæssige indikatorer omfatter gentagen rekognoscering hvor samme personer observeres flere gange uden tydelig legitim grund, usædvanlig interesse i

sikkerhedsforanstaltninger, nervøs eller mistænkelig adfærd samt forsøg på at teste sikkerhedsrespons. Fysiske indikatorer kan omfatte uautoriserede ændringer i omgivelserne, efterladte genstande eller pakker, tegn på manipulation af sikkerhedssystemer samt beskadigelse af perimeterbeskyttelse.

Eskalering og alarmering af myndigheder skal ske hurtigt og effektivt, når du identificerer situationer der kræver ekspertbistand eller myndighedsindgreb. Klare eskaleringskriterier sikrer at du ved præcis, hvornår du skal kontakte forskellige myndigheder og hvordan. Øjeblikkelig alarmering ved trusler mod liv eller ejendom omfatter aktiv skyder eller voldelig angrebssituation, bevæbnet person på området, terror- eller ekstremistaktivitet samt kidnapning eller gidselsituation. Ved øjeblikkelig fare ring straks til alarmcentralen på telefon 1-1-2, og giv klar information om situationens art, præcis lokation og antal involverede personer. Ved mindre alvorlige men stadig betydelige hændelser omfatter indbrud eller tyveri opdaget efter gerningen, hærværk eller skade på ejendom samt mistænkelig adfærd, der ikke udgør øjeblikkelig trussel, kontakter du politiets vagtcentral på telefon 1-1-4.

Koordinering med politi og beredskabstjenester under aktive situationer kræver forståelse for roller, ansvar og kommunikationsprotokoller. Når beredskabet ankommer, overtager de ansvaret for håndtering af skaderne, men din lokale viden og løbende observationer forbliver værdifulde. Politiet overtager det juridiske og operative ansvar for håndteringen af situationen. Du skal identificere dig selv og din rolle, give politiet en briefing om situationen, stille dig til rådighed for vejledning og assistance samt følge politiets instruktioner uden diskussion. Din lokale ekspertise kan være uvurderlig for beredskabet, der ikke kender området. Du skal kunne give præcis information om bygningers layout og adgangsveje, lokation af sikkerhedssystemer og værktøjer, oplysninger om personer der kan være involveret samt relevant historisk kontekst for situationen.

Evakueringsprocedurer og håndtering af større grupper kræver både forhåndsplanlægning og evnen til at reagere effektivt under pres. Evakuering af højsikkerhedsområder præsenterer unikke udfordringer da du skal balancere umiddelbar sikkerhed for mennesker med beskyttelse af

følsomme faciliteter og information. Beslutning om evakuering træffes typisk af højere myndigheder, men i øjeblikkelige faresituationer kan du være nødt til at iværksætte evakuering på eget initiativ. Kriterier for øjeblikkelig evakuering omfatter brand eller eksplosion, trusler om bombeangreb, kemisk eller biologisk fare samt strukturel fare som bygningskollaps. Kontrolleret evakuering, når tid tillader det, følger etablerede procedurer. Du skal aktivere evakueringsalarmer og kommunikationssystemer, vejlede folk til nærmeste sikre udgange, sikre at alle forlader bygningen inklusiv kontrol af toiletter og lukkede rum samt dirigere folk til udpegede samlingssteder.

Efterbehandling og debriefing efter sikkerhedshændelser er kritisk for både individuel og organisatorisk læring samt for personlig mental sundhed. Hver hændelse uanset størrelse tilbyder muligheder for forbedring af procedurer og beredskab. Umiddelbar efterbehandling i timerne efter en hændelse fokuserer på sikring af velvære for involverede personer og initial informationsindsamling. Psykologisk førstehjælp for dig selv og andre involverede omfatter sikring af grundlæggende behov som vand mad og hvile, mulighed for at tale om oplevelsen med kolleger eller professionelle samt anerkendelse af normale stressreaktioner uden at presse folk

til at dele mere end de er komfortable med. Foreløbig rapportering skal udføres så snart, det er praktisk muligt, mens detaljer stadig er friske i hukommelsen. Dokumenter en kronologisk beskrivelse af hændelsen, dine observationer og handlinger, involverede personer og myndigheder samt eventuelle skader eller tab.

Cybertrusler og Hybridkrig

I dagens sammenkoblede verden er skellet mellem fysisk og digital sikkerhed næsten forsvundet. Som højsikkerhedsvagt opererer du i et miljø hvor cybertrusler direkte påvirker fysisk infrastruktur, hvor digitale angreb kan få omfattende virkelige konsekvenser og hvor modstandere anvender hybride metoder der kombinerer traditionelle og digitale angrebsmetoder. Moderne trusselsbillede kræver at du forstår hvordan cybertrusler kan manifestere sig fysisk og hvordan du skal reagere når du observerer tegn på digitale sikkerhedshændelser.

Det moderne trusselsbillede opdeles i fem forskellige kategorier af cybertrusler. Cyberspionage har et meget højt trusselsniveau mod Danmark hvor fremmede stater udfører løbende forsøg på at stjæle følsom information fra organisationer. Som fysisk sikkerhedsvagt kan du observere tegn på cyberspionage gennem usædvanlige informationsindsamlingsaktiviteter eller personer der viser upassende interesse i IT-systemer og netværksinfrastruktur. Cyberkriminalitet udgør en konstant og stigende trussel hvor kriminelle organisationer målretter både offentlige og private infrastrukturaktører med sofistikerede angrebsmetoder. Eksempelvis er brugen Ransomware-angreb, hvor kriminelle krypterer organisationers data og kræver løsesum, blevet en epidemisk trussel mod kritisk infrastruktur. Cyberaktivisme involverer politisk motiverede hackergrupper der angriber organisationer de opfatter som modstandere af deres sag. Destruktive cyberangreb har til formål at ødelægge systemer og data snarere end at stjæle information eller afpresse penge. Cyberterrorisme hvor terrororganisationer anvender digitale angreb til at fremme deres mål forbliver en bekymring selvom det hidtil har været relativt sjældent.

Social manipulation og insidertrusler repræsenterer en af de mest alvorlige sikkerhedsrisici da disse angreb udnytter menneskelig psykologi og tillid snarere end tekniske sårbarheder. Som højsikkerhedsvagt er du ofte i frontlinjen for at identificere og forebygge disse trusler. Gennem social interaktion manipuleres mennesker til at udlevere fortrolig information eller udføre handlinger, der kompromitterer sikkerhed. Angribere udnytter menneskelige svagheder som tillid, frygt, autoritetstro eller hjælpsomhed. Almindelige sociale manipulationsteknikker omfatter phishing gennem e-mails, der ser legitime ud men indeholder links til ondsindede websider eller anmodninger om følsom information. Dette sker ved hjælp af pretexting hvor angriberen skaber et opdigtet scenario for at få offeret til at udlevere information eller give adgang. Påberåbelse af autoritet hvor angriberen udgiver sig for at være en overordnet, teknisk ekspert eller myndighedsperson for at få ofre til at efterkomme anmodninger. F at få adgang til lokaliteter bruges for eksempel tailgating, hvor en angriber følger en autoriseret person gennem en sikret dør ved at udnytte høflighed eller distraktion.

Hybride trusler og påvirkningsoperationer kombinerer militære og ikke militære midler i koordinerede kampagner for at påvirke og destabilisere målnationer. Som højsikkerhedsvagt skal du forstå hvordan disse operationer kan manifestere sig og din rolle i at identificere og rapportere mistænkelige aktiviteter. Russiske hybride operationer repræsenterer den mest omfattende og sofistikerede trussel mod dansk kritisk infrastruktur i nuværende sikkerhedsmiljø. Som beskrevet af Forsvarets Efterretningstjeneste forbereder Rusland sabotage som kan iværksættes forud for en militær konflikt med NATO med formål at sætte styrker materiel og infrastruktur ud af spil. Undersøisk infrastruktur er særligt sårbar da den er vanskeligt at beskytte og overvåge. Rusland

opdaterer løbende sine planer for at sabotere kritisk undersøisk infrastruktur i tilfælde af en eskalerende konflikt eller krig mod NATO. GPS-jamming og kommunikationsforstyrrelser bliver i stigende grad anvendt som hybride virkemidler hvor Rusland allerede nu bruger jamming af både civile og militære skibes og flys kommunikation og GPS-signaler som led i sine aktiviteter rettet mod NATO landenes militære enheder.

Samarbejde mellem fysisk og cybersikkerhed kræver tæt integration da trusler sjældent respekterer traditionelle skel mellem disse områder. Som højsikkerhedsvagt er du en kritisk komponent i denne integrerede tilgang da du ofte er den første til at observere fysiske manifestationer af digitale trusler eller digitale elementer i fysiske angreb. Integreret sikkerhedsarkitektur betyder at moderne sikkerhed kræver at fysiske og digitale sikkerhedsdomæner arbejder sammen. Informationsdeling mellem fysisk og cybersikkerhed skal ske systematisk og i realtid for at muliggøre effektiv respons på hybride trusler. Du skal forstå hvilke typer observationer der kan være relevante for cybersikkerhedsansvarlige og have klare procedurer for eskalering af potentielt digitale sikkerhedshændelser. Koordineret reaktion kræver at fysisk og digital sikkerhed kan operere sammen under kriser hvilket kan involvere fysisk sikring af kompromitterede IT-systemer, etablering af alternative kommunikationskanaler eller implementering af nedlukningsprocedurer for kritiske systemer.

Indsats ved cyberhændelser som fysisk sikkerhedsvagt fokuserer primært på observation, rapportering og støtte til cybersikkerhedspersonale frem for direkte teknisk intervention. Din rolle er at fungere som øjne og ører der kan identificere fysiske manifestationer af digitale problemer og sikre fysisk adgangskontrol under cyberhændelser. Genkendelse af cyberhændelser gennem fysiske indikatorer omfatter usædvanlige systemnedbrud eller langsom performance, uforklarlige ændringer i systemopførsel eller output, uautoriserede personer ved IT-systemer eller serverrum samt medarbejdere der rapporterer mistænkelige e-mails eller IT-problemer. Ved mistanke om cyberhændelser skal du rapportere øjeblikkeligt til både din supervisor og kundens IT sikkerhedsansvarlige, dokumentere dine observationer detaljeret samt øge overvågning af kritiske IT-områder.

Sektorspecifikke udfordringer

Som højsikkerhedsvagt vil du arbejde på tværs af forskellige sektorer og industrier hver med deres unikke sikkerhedsudfordringer, lovmæssige krav og operationelle kompleksiteter. Hver sektor har udviklet specialiserede sikkerhedsprotokoller baseret på deres særlige sårbarheder

og samfundsmæssige betydning. Din forståelse af disse sektorspecifikke krav vil gøre dig til en mere effektiv og værdifuld sikkerhedsprofessionel.

Lufthavne repræsenterer nogle af de mest komplekse sikkerhedsmiljøer der eksisterer hvor national sikkerhed møder international handel og millioner af passagerer passerer gennem dagligt. Lufthavne har vagtfunktionærer ansat til at foretage visitation af passagerer og andre sikkerhedsopgaver samt forebyggelse af terrorhandlinger. Den tredelte sikkerhedsstruktur i lufthavne omfatter landside, som er de offentligt tilgængelige områder før sikkerhedskontrol, airside, som er de sikrede områder efter sikkerhedskontrol hvor passagerer og fly befinder sig, samt kritiske operative områder som kontroltårn, bagagehåndteringssystemer og brændstofforsyning. Passagerscreening er det mest synlige element af lufthavnssikkerhed, hvor du som sikkerhedsvagt kan være involveret i visitation af passagerer og håndbagage, bedømmelse af mistænkelig adfærd gennem observationsteknikker samt håndtering af forbudte genstande og eskalering til politi.

Energisektoren udgør rygraden i moderne samfund og er derfor klassificeret som højeste prioritet under CER-loven. Som højsikkerhedsvagt i energisektoren arbejder du med at beskytte faciliteter der er absolut essentielle for samfundets funktion fordi selv kortvarige afbrydelser kan få katastrofale konsekvenser. Elproduktionsanlæg omfatter både traditionelle kulfyrede eller gasfyrede kraftværker og moderne vedvarende energianlæg som vindmølleparker og solenergianlæg. Alle disse faciliteter kræver konstant beskyttelse mod både fysiske angreb og cybertrusler. Transmissions og distributionssystemer transporterer energi fra produktionsanlæg til forbrugere gennem komplekse netværk af højspændingslinjer, transformerstationer og fordelingsstationer. Disse spredte assets er særligt sårbare da de ikke alle kan beskyttes med konstant bemanding. Din rolle som højsikkerhedsvagt ved energifaciliteter fokuserer på perimeterbeskyttelse og adgangskontrol, overvågning af kritiske anlæg og hurtig detektion af uautoriserede personer, koordinering med driftspersonale omkring sikkerhedsprocedurer samt respons på alarms og mistænkelige aktiviteter.

Datacentre og telekommunikation udgør den digitale infrastruktur som moderne samfund er fuldstændig afhængige af. Som beskrevet i CER loven omfatter digital infrastruktur både internetudvekslingspunkter, DNS-tjenesteudbydere, TLD-navneregistre samt datacentertjenester og cloud computing-tjenester der betjener kritiske funktioner. Datacentre huser den fysiske infrastruktur bag digitale tjenester og repræsenterer koncentrerede mål for både fysiske og digitale angreb. Moderne datacentre er klassificeret efter deres tier niveau der angiver deres pålidelighed og redundans hvor tier fire datacentre har højeste sikkerhedsniveau med fuldstændig redundans og tolerance over for fejl. Adgangskontrol til datacentre er ekstremt stringent med multiple verificeringslag der typisk omfatter perimeterkontrol ved indgang til bygningen, sekundær kontrol ved indgang til datacenterfaciliteter, biometrisk verificering for adgang til serverhaller samt eskortekrav for alt ikke permanent personale.

Finansielle institutioner er centrale for økonomisk stabilitet og er derfor både højværdimål for kriminelle og kritiske enheder under CER-loven. Som højsikkerhedsvagt ved finansielle institutioner skal du beskytte både fysiske værdier, digitale transaktionssystemer og fortrolig finansiel information. Banker og kreditinstitutioner har traditionelt haft omfattende fysiske

sikkerhedsforanstaltninger fokuseret på beskyttelse af kontanter og værdier samt forebyggelse af røveri. Moderne bankvirksomhed er dog primært digital hvilket betyder at cybersikkerhed er lige så kritisk som fysisk sikkerhed. Betalingstjenester og finansmarkedsinfrastruktur omfatter betalingssystemer der håndterer elektroniske transaktioner, clearingcentraler der afvikler værdipapirhandel samt andre kritiske finansielle systemkomponenter. Disse systemer håndterer enorme økonomiske værdier og deres nedbrud kan få systemiske konsekvenser for hele økonomien. Sikkerhedskrav til finansielle institutioner er omfattende og reguleret af både national lovgivning og internationale standarder hvor PCI DSS-standarden specificerer sikkerhedskrav for organisationer der håndterer betalingskortdata, anti-hvidvask regulering kræver omfattende identifikation og overvågning af kunder og transaktioner, og databeskyttelse skal sikre kunders finansielle information mod både brud og misbrug.

Arbejde som højsikkerhedsvagt på tværs af disse fire kritiske sektorer giver dig indsigt i både fælles udfordringer og sektorspecifikke kompleksiteter. Alle sektorer deler bekymringer om cybertrusler, interne trusler og behovet for modstandsdygtighed mod både naturkatastrofer og menneskeskabte trusler. Teknologisk integration er et gennemgående tema hvor traditionel fysisk sikkerhed bliver sammenkoblet med cybersikkerhed og automatiseringssystemer. Kontinuerlig læring er nødvendigt da trusselsbilledet udvikler sig konstant og nye teknologier skaber både muligheder og sårbarheder. Som højsikkerhedsvagt skal du være forpligtet til løbende faglig udvikling og opmærksomhed på både sektorspecifikke tendenser og generelle sikkerhedsudviklinger.

Dette kompendium har gennemgået de fundamentale principper, færdigheder og procedurer der er nødvendige for at fungere effektivt som højsikkerhedsvagt. Fra forståelse af kritisk infrastruktur og dit juridiske ansvar til praktiske færdigheder i observation, adgangskontrol og krisehåndtering har du nu et omfattende fundament for professionelt sikkerhedsarbejde. Husk at kontinuerlig træning og udvikling er afgørende i denne dynamiske profession hvor trusler konstant udvikler sig. Din rolle som højsikkerhedsvagt er afgørende for beskyttelsen af samfundets kritiske funktioner, og gennem professionel udførelse af dit arbejde bidrager du direkte til Danmarks sikkerhed og modstandsdygtighed.

Ordforklaring

ACL Access Control List (Adgangskontrolliste)

AIA Automatisk Indbrudsalarmeringsanlæg

AP Alarmpatrulje

ASIS American Society for Industrial Security (nu ASIS International) - International sikkerhedsorganisation

BTA Behavioral Threat Assessment (Adfærdsbaseret trusselsvurdering)

BTAM Behavioral Threat Assessment and Management (Adfærdsbaseret trusselsvurdering og -håndtering)

CCTV Closed-Circuit Television (Lukket kredsløbs-tv/overvågningskamera)

CER Critical Entities Resilience (Kritiske enheders modstandsdygtighed)

CFCS Center for Cybersikkerhed (Dansk myndighed under Forsvarets Efterretningstjeneste)

CPP Certified Protection Professional (Certificeret sikkerhedsprofessionel)

CPTED Crime Prevention Through Environmental Design (Kriminalitetsforebyggelse gennem miljødesign)

DHS Department of Homeland Security (USA's indenrigsministerium)

ETA Estimated Time of Arrival (Forventet ankomsttid)

EU Den Europæiske Union

FACS Facial Action Coding System (System til kodning af ansigtsudtryk)

FE Forsvarets Efterretningstjeneste

GDPR General Data Protection Regulation (Databeskyttelsesforordningen)

HR Human Resources (Personaleafdeling)

HVAC Heating, Ventilation, and Air Conditioning (Varme, ventilation og aircondition)

ICAO International Civil Aviation Organization (International organisation for civil luftfart)

ID Identification (Identifikation)

IED Improvised Explosive Device (Improviseret sprængladning)

ISMS Information Security Management System (Informationssikkerhedsledelsessystem)

ISO International Organization for Standardization (International standardiseringsorganisation)

ISPS International Ship and Port Facility Security (International sikkerheds-kode for skibe og havne)

KPI Key Performance Indicator (Nøglepræstationsindikator)

LBK Lovbekendtgørelse

NIS Network and Information Security (Netværks- og informationssikkerhed)

OODA Observe, Orient, Decide, Act (Observer, Orienter, Beslut, Handl - beslutningsmodel)

PAP Physical Asset Protection (Fysisk aktivbeskyttelse)

PCI DSS Payment Card Industry Data Security Standard (Sikkerhedsstandard for betalingskortindustrien)

PET Politiets Efterretningstjeneste

QR Quick Response (Hurtig respons - ofte brugt om QR-koder)

RACE Rescue, Alarm, Contain, Evacuate/Extinguish (Red, Alarmer, Indeslut, Evakuer/Sluk brand)

ROI Return on Investment (Investeringsafkast)

SOP Standard Operating Procedure (Standardprocedure)