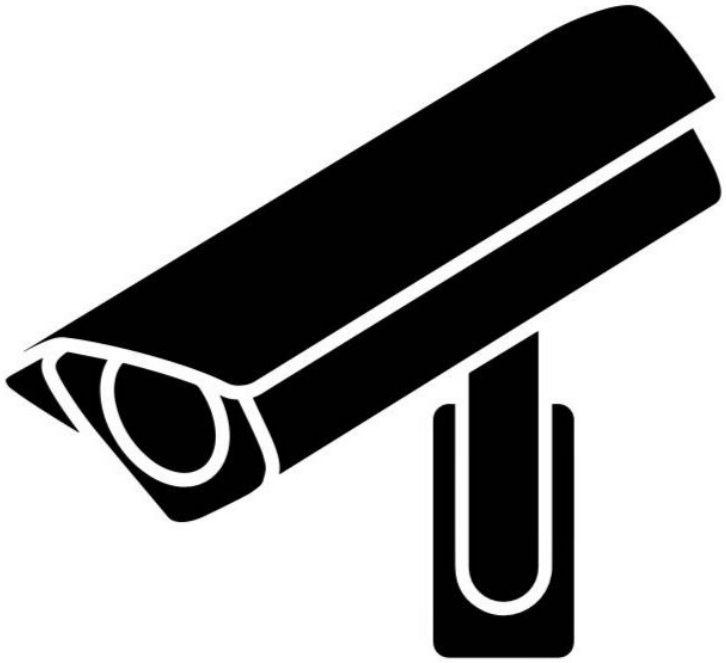


KAMERABEVAKNING

EN ÖVERGRIPANDE GUIDE FÖR FÖRETAG

PRUDENCIA
SECURITY

www.prudsec.se

Innehåll

Inledning 3
1. Arbeta preventivt 4
1.1 Vad innebär preventivt arbete med kamerasystem? 4
1.2 Förutsättningar 4
1.3 Exempel 5
1.4 Utmaningar 6
2. On premise eller molnbaserade system 7
2.1 On premise 7
2.2. Molnbaserade system 7
2.3 Hybridlösningar 8
3. Analysfunktioner 9
4. Val av kamera 12
4.1 Kameratyper 12
4.2 Viktiga funktioner att beakta vid val av kamera 13
5. Sensorer 15
5.1 Sensorernas roll 15
5.2 Integrationsmöjligheter 15
6. Federerade system för centraliserad hantering 16
6.1 Fördelar med federerade system 16
6.2 Typiska funktioner i federerade system 17
7. Integration mot larmcentral 19
7.1 Närvaro 24/7 19
7.2 Rätt åtgärd 19
7.3 Avskräck och agera 19
8. GDPR och NIS2 20
8.1 Vad är GDPR och NIS2? 20
8.2 Krav på GDPR-efterlevnad vid kameraövervakning 20
8.3 Krav på NIS2-efterlevnad vid kameraövervakning 21
8.4 Samordning mellan GDPR och NIS2 22
9. CER-direktivet 23
9.1 Vad är CER-direktivet och varför är det viktigt? 23
9.2 En initial strategi för efterlevnad 23
10. Upphandling 24

Inledning

Kamerasystem är idag en nyckelkomponent för att skapa trygga och effektiva miljöer inom både privat och offentlig sektor. Den teknologiska utvecklingen har förvandlat dessa system från passiva övervakningsverktyg till aktiva lösningar som kan analysera, upptäcka och larma om avvikelser i realtid.

Kärnan i ett modernt kamerasystem är en VMS-plattform (Video Management System), som hanterar videoströmmar, lagring och analys. VMS möjliggör även integration med andra system och kan installeras antingen som en del av befintliga IT-miljöer med AD-integration och domänanslutning, eller som ett fristående system. Detta ställer höga krav på både cybersäkerhet och systemarkitektur.

Kameror, detektorer och IoT-sensorer placeras strategiskt för att möta de specifika behoven på varje plats. Idag fungerar kameror inte bara som traditionella övervakningsverktyg utan även som avancerade sensorer för datorseende (computer vision). Med hjälp av AI-analys kan dessa system tillämpas på en mängd områden utöver säkerhet, såsom att optimera verksamhetsprocesser, förbättra kundupplevelser och stödja hållbarhetsmål.

För att möjliggöra dessa funktioner är det avgörande att välja ett framtidssäkert VMS som kan hantera komplex metadata och anpassas till nya användningsområden. Ett modernt kamerasystem kan också hantera realtidslarm, vilket möjliggör snabba och effektiva åtgärder. Larm kan skickas direkt till exempelvis medarbetare eller en auktoriserad larmcentral för omedelbar respons. Denna funktion bidrar inte bara till ökad säkerhet utan även till förbättrad flexibilitet och effektivitet i hanteringen av olika situationer.

Ett framtidssäkert system kan även användas för fjärrstyrning av funktioner. Exempelvis kan en larmcentral övervaka inpasseringar, kommunicera via porttelefon och styra grindar eller andra IoT-enheter på distans. Genom att samla in och analysera data bidrar moderna kamerasystem till bättre beslutsunderlag och på så sätt en mer lönsam verksamhet.

Kombinationen av säkerhet, avancerad analys och anpassningsbarhet gör dessa system till en central del av både dagens och framtidens lösningar för trygghet och verksamhetsoptimering.

Denna guide syftar till att ge en tydlig och lättförståelig översikt av hur moderna kamerasystem fungerar samt erbjuda vägledning i att välja, integrera och optimera system som både förbättrar säkerheten och stärker verksamheten.

1. Arbeta preventivt

Ett av de mest värdefulla användningsområdena för moderna kamerasystem är möjligheten att arbeta preventivt – att förebygga incidenter innan de inträffar.

Genom att kombinera kameraövervakning med videoanalys och proaktiva arbetsprocesser kan organisationer inte bara hantera säkerhet utan också optimera resurser och minimera risker.

1.1 Vad innebär preventivt arbete med kamerasystem?

Preventivt arbete handlar om att använda kamerateknologi och dataanalys för att identifiera potentiella risker och vidta åtgärder innan en händelse eskalerar till ett problem. Det kan inkludera allt från att upptäcka ovanligt beteende till att förhindra bränder eller skadegörelse.

Exempel på tillämpningar:

- Identifiera misstänkta rörelser vid känsliga områden.
- Tidigt upptäcka värmeutveckling eller andra indikationer på brandrisk.
- Övervaka kundflöden i butiker för att undvika trängsel och förbättra service.

1.2 Förutsättningar

Teknologiska förutsättningar

- **Kameror:** Kameror med hög upplösning, termisk avbildning eller rörelsedetektion är centrala för preventivt arbete. Exempelvis kan termiska kameror användas för att upptäcka bränder innan de syns med blotta ögat, förutsatt att inget döljer värmesignaturen.
- **Sensorer:** I kombination med kameror kan även annan teknik, såsom radar, lidar och rörelsesensorer, användas för att skapa innovativa och effektiva larmlösningar.
- **Realtidsanalys:** System eller kameror som kan analysera videoströmmar i realtid är avgörande för att snabbt identifiera avvikelser och generera larm.

- **Automatiserade larm:** Funktioner som automatiskt skickar varningar till ansvariga eller till en extern larmcentral när avvikande beteenden eller faror upptäcks.

Integrerade system

- Ett effektivt preventivt system fungerar inte isolerat. Genom integration med andra säkerhetssystem, såsom passerkontroll, larmsystem och IoT-enheter, kan kamerateknologin spela en nyckelroll i att skapa en helhetslösning.
- Exempelvis kan en kamera upptäcka en obehörig person och automatiskt låsa dörrar och larma säkerhetspersonal.

Data och analys

- **Deep learning och machine learning/AI:** Dessa teknologier kan tränas för att känna igen mönster och identifiera ovanliga beteenden, som att någon uppehåller sig nära ett känsligt område eller att en olycka verkar vara på väg att ske.
- **Prediction models:** Genom att analysera tidigare händelser kan systemet lära sig att förutse liknande incidenter och agera innan de sker.

Personal och rutiner

- Preventivt arbete kräver att personal är utbildad i att förstå och tolka data från kameror och analysverktyg.
- Rutiner bör finnas för att snabbt agera på larm och varningar, exempelvis genom att dirigera säkerhetspersonal eller vidta andra åtgärder.

1.3 Exempel

Allmänna platser

- Kameraövervakning i stadskärnor kan identifiera folksamlingar som riskerar att leda till konflikter. Genom att larma polisen tidigt kan insatser sättas in innan en situation eskalerar.

Lager och skog

- Termiska kameror kan identifiera värmesignaturer som indikerar bränder. I lagerlokaler kan det rädda stora ekonomiska värden, medan i skogar kan det bidra till att skydda miljön.

Butiker

- Genom att analysera kundrörelser kan butikspersonal förebygga trängsel och förbättra kundupplevelsen samt säkerheten. Historisk data kan också användas för att optimera bemanning.

Kritisk infrastruktur

- Övervakning av broar, tunnlar och andra infrastrukturer kan bidra till att potentiella problem som sprickor eller strukturella avvikelser upptäcks innan de leder till större skador.

1.4 Utmaningar

Kostnad

- Avancerade kameror och analysverktyg innebär initialt högre investeringar. Det är viktigt att kalkylera avkastning på investeringen genom att beakta kostnadsbesparingar från förebyggda incidenter.

Dataskydd

- GDPR och andra dataskyddsregler måste följas, särskilt när preventivt arbete innebär insamling och analys av stora datamängder.

Teknisk komplexitet

- Att integrera kameror med andra system kan vara tekniskt utmanande och kräver expertis både under implementering och drift.

Falsklarm

- Systemet bör vara väl kalibrerat för att minimera falsklarm, vilket annars kan leda till resursförbrukning och minskat förtroende för teknologin. Definiera övervakade områden noggrant för att undvika att irrelevanta rörelser larmar.

2. On premise eller molnbaserade system

När det kommer till avancerade kamerasystem är valet mellan on-premise och molnbaserade lösningar en av de mest centrala frågorna att besvara under upphandlingsprocessen. Varje alternativ har sina unika fördelar och nackdelar, och valet bör baseras på organisationens behov, säkerhetskrav och långsiktiga strategi.

2.1 On premise

Ett on-premise-system innebär att all data och all programvara lagras och hanteras på plats inom organisationens egna servrar och nätverk. Detta alternativ ger hög kontroll och säkerhet, vilket gör det attraktivt för verksamheter som hanterar känslig information eller har strikta krav på dataintegritet.

Fördelar med On premise:

- Kontroll: Fullständig äganderätt över data, mjukvara och hårdvara.
- Säkerhet: All data stannar inom organisationens egna nätverk, vilket minimerar risken för dataläckage via tredje part.
- Stabilitet: Ingen beroendeställning till internetanslutning för att komma åt systemet.
- Anpassning: Kan anpassas till unika behov utan att begränsas av molntjänsternas standardfunktioner.

Nackdelar med On premise:

- Initialkostnad: Kräver investeringar i infrastruktur och hårdvara.
- Underhåll: Organisationen måste själv hantera uppdateringar och tekniskt underhåll.

2.2. Molnbaserade system

Molnbaserade system bygger på att både data och mjukvara hanteras via externa datacenter som nås via internet. Detta alternativ erbjuder flexibilitet och snabb skalbarhet.

Fördelar med molnbaserade system:

- Kostnadseffektivitet: Lägre initial kostnad eftersom ingen omfattande lokal infrastruktur behövs. Beroende på fall kan den långsiktiga kostnaden överstiga den initiala besparingen.
- Skalbarhet: Systemet kan snabbt anpassas för att hantera fler kameror.
- Tillgänglighet: Systemet är tillgängligt från vilken plats som helst med en internetuppkoppling.
- Automatiserade uppdateringar: Leverantören ansvarar för att hålla mjukvaran uppdaterad.

Nackdelar med molnbaserade system:

- Beroende av internet: Systemets prestanda är direkt kopplat till kvaliteten på internetuppkopplingen.
- Dataskydd: Kräver noggrann granskning av molnleverantörens dataskyddsåtgärder för att säkerställa GDPR-efterlevnad samt NIS2.
- Långsiktiga kostnader: Prenumerationsmodeller kan leda till högre kostnader över tid jämfört med en on-premise-lösning.

2.3 Hybridlösningar

För organisationer som behöver balans mellan kontroll och flexibilitet kan en hybridlösning vara det bästa alternativet. Här lagras kritisk data lokalt medan mindre känslig data hanteras i molnet, vilket ger högre säkerhet utan att kompromissa med skalbarheten.

Fördelar med hybridlösningar:

- Flexibilitet: Kombinationen av lokalt lagrad data och molnlagring kan optimeras för specifika behov.
- Bandbredd optimeras genom att kombinera lagring lokalt och i molnet. Vilket ökar hastigheten och sparar kostnader.
- Riskminimering: Kritiska system och data hålls skyddade på plats, medan molnet används för redundans och skalbarhet.
- Effektivitet: Delad belastning mellan lokal och molnbaserad infrastruktur.

3. Analysfunktioner

Moderna kamerasystem har utvecklats långt bortom enkel övervakning. Analysfunktioner gör det möjligt att automatisera övervakning, identifiera risker och skapa mervärde genom att generera användbara insikter för både säkerhetsarbete och affärsstrategier. Dessa funktioner bygger på avancerad AI och maskininlärning, som kan upptäcka och analysera mönster i videoströmmar.

Perimeterövervakning

Perimeterövervakning är en av de mest grundläggande analysfunktionerna, och den används för att identifiera intrång på skyddade områden. Genom att skapa virtuella gränser (geofencing) kan systemet automatiskt larma när någon korsar dessa gränser.

Exempel på användningsområden:

- Skydd av byggarbetsplatser, kritisk infrastruktur och lagerområden.
- Detektion av obehörig tillgång till parker eller privata fastigheter.

Loiteringdetektion

Loiteringdetektion är utformad för att identifiera individer eller fordon som vistas för länge på en viss plats utan uppenbar anledning. Detta kan indikera potentiella hot, såsom förberedelse för brott eller sabotage.

Exempel på användningsområden:

- Förhindra obehöriga att planera inbrott eller vandalism.
- Identifiera misstänkt beteende vid entréer eller känsliga områden.

Kvarlämnade föremål (left item detection)

Denna funktion används för att upptäcka föremål som lämnas kvar på en plats under en viss tid. Detta är särskilt viktigt för säkerhetsövervakning i offentliga miljöer där kvarlämnade föremål kan utgöra en säkerhetsrisk.

Exempel på användningsområden:

- Upptäcka misstänkta föremål på flygplatser, tågstationer och köpcentrum.
- Larma om övergivna väskor eller paket.

Branddetektering

Termiska kameror i kombination med analysmjukvara kan upptäcka brand eller ökad värmeutveckling innan traditionella brandlarm aktiveras. Detta möjliggör tidiga åtgärder och kan rädda både liv och egendom.

Exempel på användningsområden:

- Upptäcka bränder i skogar, lager eller fabriker.
- Larma om ovanliga temperaturökningar i riskområden.

Kundbeteendeanalys

Utöver säkerhet används kamerasystem idag allt oftare för att analysera kundbeteenden i detaljhandeln. Genom att följa rörelsemönster och identifiera populära områden i butiker kan man optimera produktplacering och kundflöde.

Exempel på användningsområden:

- Spåra vilka områden i en butik som drar mest uppmärksamhet.
- Optimera bemanning baserat på kundflöden.

Unusual behavior detection

AI-drivna system kan upptäcka avvikande beteenden som kan signalera potentiella säkerhetsrisker. Detta inkluderar oväntade rörelsemönster, ovanligt långvarig aktivitet eller andra avvikelser.

Exempel på användningsområden:

- Identifiera misstänkta rörelser i parkeringsgarage.
- Detektera farligt beteende vid maskiner eller högriskområden.

Fördelar med integrerad analys

Automatisering: Systemet larmar automatiskt vid avvikelser, vilket minskar behovet av manuell övervakning.

Resurseffektivitet: Personalens tid frigörs för att fokusera på mer kritiska uppgifter.

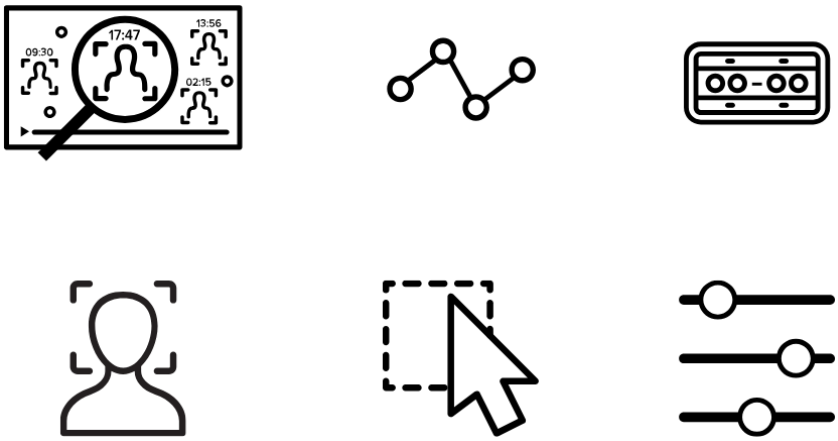
Datadrivna beslut: Analysdata kan användas för att optimera affärs- eller säkerhetsstrategier.

Proaktivitet: Tidig upptäckt av risker möjliggör förebyggande åtgärder.

Utmaningar

Kostnad: Analysfunktioner kan öka systemets totala kostnad.

Dataskydd: Insamlad data måste hanteras enligt GDPR och andra dataskyddsregler.



4. Val av kamera

Valet av kameror är en av de mest avgörande delarna vid upphandling av ett kamerasystem. Rätt kameror säkerställer att systemet kan leverera de resultat som verksamheten behöver, oavsett om det handlar om säkerhet, övervakning eller analys. Kameror är inte en "one size fits all"-lösning; olika typer av kameror är optimerade för olika miljöer och funktioner.

4.1 Kameratyper

Fasta kameror

- Funktion: En fast kamera är stationär och riktad mot en specifik plats eller vinkel.
- Fördelar: Låg kostnad, enkel installation och idealisk för områden som inte kräver rörlig övervakning.
- Exempel på användning: Entréer, korridorer, betalstationer.

PTZ-kameror (Pan-Tilt-Zoom)

- Funktion: PTZ-kameror kan fjärrstyras för att panorera, luta och zooma in på objekt.
- Fördelar: Flexibilitet att övervaka stora områden eller zooma in för detaljerad bild.
- Exempel på användning: Stora utomhusområden, arenor, parkeringsplatser.

Termiska kameror

- Funktion: Termiska kameror använder värmesignaturer istället för synligt ljus för att skapa en bild.
- Fördelar: Fungerar i mörker, genom dimma och rök; idealisk för detektering av värmeutveckling.
- Exempel på användning: Branddetektering, perimeterskydd, industriella tillämpningar.

Fisheye-kameror

- Funktion: Fisheye-kameror ger en 360-graders vy av ett område utan att behöva flera kameror.
- Fördelar: Täckning av stora områden utan blinda fläckar.
- Exempel på användning: Kontorslokaler, receptioner, konferensrum.

Multisensorkameror

- Funktion: Kameror med flera sensorer som kan övervaka flera riktningar samtidigt.
- Fördelar: Effektivt för att täcka stora områden med färre enheter.
- Exempel på användning: Stora torg, shoppingcenter, logistikcentraler.

4.2 Viktiga funktioner att beakta vid val av kamera

Upplösning

- Högre upplösning ger skarpare bilder och möjliggör detaljerad analys, särskilt viktigt för ansiktsigenkänning eller fordonsidentifiering.
- Exempel: 4K-kameror för platser där detaljer är avgörande, som entréer eller kassa miljöer.

Ljusförhållanden

- Kameror med low-light-teknologi kan ge högkvalitativa bilder i svagt ljus.
- Kameror med IR-belysning kan ge tydliga bilder även i totalt mörker.
- Exempel: Utomhuskameror vid svagt belysta områden.

Hållbarhet och klimatanpassning

- Kameror som används utomhus måste tåla tuffa väderförhållanden, såsom regn, snö och extrem värme eller kyla.
- Kameror med IP-klassificering (exempelvis IP66 eller IP67) och vandalskydd (IK-klassificering) är att föredra.

Stabilisering

- Kameror med stabilisering för att undvika skakiga bilder vid rörelse.
- Viktigt för områden med vibrationer, som broar eller fordon.

Integrationsmöjligheter

- Kameran bör stödja standardprotokoll, såsom ONVIF, för att möjliggöra integration med olika VMS-plattformar och analysverktyg. En fördel är om kameran även stöder ONVIF Profil M, vilket gör det möjligt att integrera metadata i VMS-systemet.

Lagringslösningar

- Kameror med stöd för edge-lagring (SD-kort) kan spara videomaterial lokalt som backup om nätverket går ner.

Fallgropar att undvika

Överinvestering: Att välja kameror med högre kapacitet än vad som behövs kan öka kostnaderna utan att tillföra värde.

Underinvestering: Billiga kameror med dålig bildkvalitet kan göra systemet ineffektivt och omöjligt att använda för analys eller bevisföring. Samt att billigare kameror kan ha mindre säkerhetsfunktioner och sämre ex. IR belysning.

Brist på kompatibilitet: Kameror som inte följer standardprotokoll kan begränsa flexibiliteten och integrationen i framtiden.

5. Sensorer

Moderna VMS kan hantera mer än bara videoströmmar. Genom att använda öppna system och standardprotokoll som ONVIF blir det möjligt att integrera en mängd andra typer av sensorer. Detta tillför ett djup och en bredd i övervakningen som kan skapa mervärde inom både säkerhet och verksamhetsoptimering.

5.1 Sensorernas roll

Förbättrad riskhantering: Sensorer som rörelsedetektorer, ljudsensorer, vibrationssensorer och luftkvalitetssensorer kan samverka med VMS för att detektera avvikelser. Exempelvis kan en ljudsensor upptäcka glas som krossas och aktivera en kamera i närheten för att spela in händelsen.

Proaktiv säkerhet: Temperatur- och fuktsensorer kan identifiera miljöförändringar som tyder på brandrisk eller vattenläckage. Dessa sensorer kan trigga åtgärder i realtid, som att aktivera larm eller skicka notifikationer till säkerhetspersonal.

Verksamhetsoptimering: Rörelsesensorer i lager kan effektivisera logistik och arbetsflöden genom att spåra aktivitet och generera insikter som förbättrar planeringen.

5.2 Integrationsmöjligheter

1. ***IoT- enheter:*** Ett öppet VMS kan integreras med IoT-enheter, vilket möjliggör samordning mellan olika system. Till exempel kan en rörelsesensor i ett passersystem både aktivera en kamera och låsa dörrar för att begränsa tillgången.
2. ***Standardisering och skalbarhet:*** Genom att använda öppna protokoll och API:er kan sensorer från olika tillverkare anslutas. Detta gör systemet skalbart och framtidssäkert.

6. Federerade system för centraliserad hantering

I ett federerat system kopplas flera självständiga kamerasystem samman och hanteras via den centrala managementservern.

Varje system bibehåller sin autonomi men kan integreras för att ge en övergripande vy och samordnad hantering i ett enda gränssnitt. Detta gör det möjligt för organisationer med många anläggningar – exempelvis skolor, sjukhus eller kontor – att övervaka och administrera hela sitt nätverk från en central plats.

Genom att samla alla delar av kamerasystemet i en enhetlig plattform kan användare uppnå högre effektivitet, bättre skalbarhet och ökad kontroll.

6.1 Fördelar med federerade system

Centraliserad hantering

- Alla kameror och inspelningar kan administreras från en central inloggningspunkt.
- Enkel åtkomst till livevideo, historiska inspelningar och systeminställningar.
- Minskad komplexitet för administratörer och användare.

Effektivitet

- Personal behöver inte vara fysiskt närvarande på varje plats för att övervaka eller hantera kamerorna.
- Enklare hantering av uppdateringar och konfigurationer, vilket sparar tid och resurser.

Skalbarhet

- Systemet kan enkelt utökas med nya kameror, platser eller funktioner utan att behöva ändra den befintliga strukturen.
- Passar både små organisationer som växer och stora verksamheter som vill konsolidera sina system.

Ökad kontroll och säkerhet

- Administratörer kan definiera och hantera användarbehörigheter centralt.

- Åtkomstkontroller kan säkerställa att endast auktoriserade personer har tillgång till specifika kameror eller funktioner.

Flexibilitet för olika behov

- Möjlighet att integrera olika kameratyper och leverantörer i samma system.
- Anpassningsbar för olika verksamhetsbehov, från säkerhetsövervakning till affärsanalys.

6.2 Typiska funktioner i federerade system

Enhetlighet

- Ett intuitivt gränssnitt som gör det enkelt att navigera mellan olika platser och kameror.
- Gemensamma standarder och protokoll för att minimera kompatibilitetsproblem.

Automatisering

- Automatiska larm och notifieringar vid avvikelser, oavsett var i systemet de inträffar.
- Central hantering av schemalagda uppgifter som uppdateringar och säkerhetskopiering.

Översikt och rapporter

- Möjlighet att generera centraliserade rapporter om systemets prestanda, händelser och analyser.
- Dashboard-lösningar för att visualisera status och aktiviteter i realtid.

Säker drift

- Systemet fortsätter fungera lokalt vid nätverksavbrott, och data synkroniseras till den centrala plattformen när anslutningen återställs.
- Möjlighet till redundans genom backup-servrar.

Utmaningar med federerade system

Komplex implementation

- Att koppla samman flera system kräver noggrann planering och expertkunskap.
- Integration mellan äldre och nyare system kan vara tekniskt krävande.

IT-säkerhet

- Federerade system behöver ett starkt skydd mot cyberhot, eftersom en attack på central nivå kan påverka hela nätverket.
- Kryptering och robusta autentiseringslösningar är nödvändiga.

Kostnad

- Initiala kostnader för att etablera en federerad struktur kan vara högre jämfört med enklare lösningar.

Exempel på användningsområden

Kommuner

- Övervakning av skolor, bibliotek och offentliga byggnader med central hantering för kommunens säkerhetsavdelning.

Företagskoncerner

- Kameranätverk för kontor, lager och fabriker kan hanteras globalt från en central plats.

Transport och infrastruktur

- Federerade system används ofta för att övervaka stora infrastrukturer som flygplatser, järnvägsnät och hamnar.

7. Integration mot larmcentral

Genom att koppla VMS till larmcentralens system kan operatörerna få direkt åtkomst till realtidsvideo, högupplösta inspelningar och kritiska sensordata.

Detta möjliggör snabb respons på larm, där rätt åtgärder kan vidtas direkt. Integration ger också möjlighet att fjärrstyra funktioner som grindar, högtalare och andra IoT-enheter.

7.1 Närvaro 24/7

Ett kamerasystem som är integrerat med en extern larmcentral ger konstant övervakning av ett område eller fastighet. Med avancerad teknik som videoanalys, markradar, lidar och värmekameror upptäcks obehöriga intrång i realtid. Larmcentralens operatörer agerar direkt, oavsett tid på dygnet, vilket garanterar en trygg och säker miljö för verksamheten.

7.2 Rätt åtgärd

En av de största fördelarna med att koppla ett VMS till en larmcentral är att rätt åtgärd kan vidtas i exakt rätt ögonblick. När ett larm utlöses får operatörerna en tydlig bild av situationen via högupplösta kamerabilder och annan sensordata. Utifrån detta kan de:

- Tillkalla polis, väktare eller räddningstjänst.
- Guida insatser för att säkra platsen eller gripa förövare.
- Undvika onödiga utryckningar genom att verifiera larm.

7.3 Avskräck och agera

Ett integrerat system möjliggör tvåvägskommunikation via högtalare, vilket är ett kraftfullt sätt att hantera incidenter. Operatörerna kan:

- Informera obehöriga om att lämna området.
- Använda skarpa varningar eller förinspelade meddelande som avstyr pågående skadegörelse eller inbrott.

Denna funktion skapar en aktiv och avskräckande effekt som traditionella larm inte kan matcha.

8. GDPR och NIS2

Efterlevnad av lagar och regler är en central aspekt vid upphandling och användning av moderna kamerasystem. För organisationer som verkar inom EU är det särskilt viktigt att följa både GDPR (General Data Protection Regulation) och NIS2-direktivet (Network and Information Security Directive). Dessa regler har olika syften men tillsammans säkerställer de att data hanteras på ett säkert, lagligt och ansvarsfullt sätt.

8.1 Vad är GDPR och NIS2?

GDPR – Skydd av Personuppgifter GDPR reglerar hur personuppgifter ska hanteras och skyddas inom EU. När det gäller kameraövervakning omfattas videomaterial, eftersom det kan innehålla identifierbara personer, fordon eller annan personrelaterad data. Syftet med GDPR är att stärka individens rätt till integritet och säkerställa att organisationer hanterar data på ett transparent och ansvarsfullt sätt.

NIS2 – Cybersäkerhet för Samhällskritiska Funktioner NIS2-direktivet är en uppdatering av det ursprungliga NIS-direktivet och syftar till att förbättra cybersäkerheten i samhällsviktiga sektorer och leverantörskedjor. Detta innebär att organisationer som hanterar kameraövervakning måste säkerställa att deras system är motståndskraftiga mot cyberhot och att de har mekanismer på plats för att upptäcka, hantera och rapportera säkerhetsincidenter.

8.2 Krav på GDPR-efterlevnad vid kameraövervakning

Transparens och skyltning

- Informera tydligt om att övervakning sker, exempelvis genom skyltar vid övervakade områden.
- Beskriv syftet med övervakningen, vilka som har åtkomst till materialet och hur länge det lagras.

Begränsning av syfte och lagring

- Data får endast samlas in och användas för specifika och legitima ändamål, såsom säkerhet eller brottsförebyggande.
- Lagringsperioden ska begränsas till vad som är nödvändigt för ändamålet.

Individers rättigheter

- Organisationer måste kunna tillhandahålla inspelningar till personer som begär att få se vilka data som lagrats om dem.
- Möjlighet till radering av data ska finnas, om det inte strider mot andra lagkrav (exempelvis för utredningar).

Säkerhet och behörighet

- Videomaterial ska skyddas genom kryptering, behörighetskontroll och loggning av åtkomst.
- Använd funktioner som anonymisering och maskering vid inspelning i känsliga områden.

8.3 Krav på NIS2-efterlevnad vid kameraövervakning

Cybersäkerhet

- Kamerasystemet måste vara skyddat mot cyberattacker genom robusta säkerhetsåtgärder som brandväggar, nätverkssegmentering och krypterad kommunikation.
- Säkerhetspatchar och uppdateringar måste implementeras regelbundet.

Incidenthantering

- Organisationer måste ha en plan för att upptäcka, hantera och rapportera säkerhetsincidenter kopplade till kameraövervakningen.
- Detta inkluderar att ha loggningsfunktioner och säkerhetskopior för att snabbt kunna återställa systemet efter en incident.

Leverantörssäkerhet

- Alla leverantörer av kamerautrustning och VMS-plattformar måste granskas för att säkerställa att de följer cybersäkerhetskrav.
- Tredjepartsrisker ska hanteras genom avtal och regelbunden revision.

Rapporteringsskyldighet

- Om en incident inträffar som kan påverka kameraövervakningens funktion eller integritet, måste den rapporteras till relevanta myndigheter inom en specificerad tidsram.

8.4 Samordning mellan GDPR och NIS2

GDPR och NIS2 är tätt sammankopplade när det gäller kameraövervakning, eftersom säker hantering av personuppgifter förutsätter att systemen är skyddade mot cyberhot. Exempelvis kan ett dataintrång som avslöjar videomaterial både vara ett brott mot GDPR och en rapporteringspliktig incident enligt NIS2.

Några nyckelaspekter för att uppfylla båda regelverken:

- Implementera en dataskyddsstrategi som kombinerar tekniska och organisatoriska åtgärder för att skydda videodata.
- Genomför regelbundna riskbedömningar och säkerhetsrevisioner av både kamerainfrastruktur och datalagring.
- Utbilda personal om krav och riktlinjer för dataskydd och cybersäkerhet.

Exempel på efterlevnad i praktiken

Offentlig verksamhet

- En kommun installerar kameraövervakning för skolor och parker. Genom tydlig skyltning och regelbundna DPIA-rapporter (Data Protection Impact Assessments) uppfyller de GDPR-kraven, medan redundanta nätverk och kryptering säkerställer NIS2-efterlevnad.

Kritisk infrastruktur

- Ett energibolag använder kameror för att övervaka anläggningar. Kamerasystemet är isolerat från företagets interna nätverk för att minimera cyberrisker, vilket följer NIS2, och all inspelning sker enligt GDPR regler för lagring och tillgång.

9. CER-direktivet

9.1 Vad är CER-direktivet och varför är det viktigt?

CER-direktivet (“Directive on the Resilience of Critical Entities”) är en EU-lagstiftning som trädde i kraft i december 2022. Det är utformat för att skydda samhällsviktiga verksamheter inom sektorer som energi, transporter, hälso- och sjukvård, dricksvattenförsörjning, digital infrastruktur, offentlig förvaltning.

Genom att säkerställa deras motståndskraft mot både fysiska och digitala hot, som naturkatastrofer, sabotage eller cyberattacker, bidrar direktivet till att upprätthålla grundläggande samhällsfunktioner.

Direktivet kräver att kritiska entiteter implementerar riskstrategier som inkluderar:

- Regelbundna riskbedömningar.
- Kontinuitetsplaner för att hantera störningar.
- Implementering av tekniska och organisatoriska skyddsåtgärder.
- Genomförande av tester och övningar för att säkerställa beredskap.

9.2 En initial strategi för efterlevnad

Kartläggning av verksamhetens kritiska funktioner: Identifiera vilka delar av er verksamhet som kan påverkas av CER och vilka potentiella risker som finns.

Genomför en riskbedömning: Bedöm sårbarheter och skapa en översikt över hot, både interna och externa.

Implementera en kontinuitetsplan: Planera för hur verksamheten kan upprätthållas vid avbrott eller kriser under olika scenarier.

Utvärdera tekniska system: Se över era befintliga säkerhetslösningar. Kamerasystem och VMS-plattformar kan spela en central roll genom att:

- Identifiera hot i realtid via videoanalys och automatiska larm.
- Säkerställa redundans: Molnbaserad och lokal lagring skyddar kritisk data.
- Integreras med andra säkerhetssystem för att skapa en helhetslösning.

Utbilda personal: En väl informerad personalstyrka är avgörande för att snabbt och effektivt hantera incidenter.

10. Upphandling

Vid upphandling av kamerasystem är det avgörande att ställa tydliga och genomtänkta funktionskrav som säkerställer att systemet inte bara uppfyller dagens behov utan också är skalbart och flexibelt för framtida användning. Genom att inkludera krav som stödjer centraliserad hantering, avancerad videoanalys och integration med andra system skapas förutsättningar för en långsiktig och kostnadseffektiv lösning.

Dessa krav underlättar inte bara valet av tekniska lösningar utan hjälper också organisationen att uppfylla regelverk som GDPR och NIS2, vilket är centralt för säker hantering av data och skydd mot cyberhot. Med rätt funktionskrav kan upphandlingsprocessen förenklas samtidigt som möjligheterna för effektiv drift, säkerhet och framtida anpassning optimeras.

Kravspecifikation för Video Management System (VMS)

1. *Systemarkitektur och skalbarhet*

- Systemet ska vara modulärt och stödja en federerad arkitektur för att möjliggöra skalbarhet till flera geografiska platser.
- Det ska kunna hantera från ett fåtal till stor mängd kameror med bibehållen prestanda och effektivitet genom att möjliggöra skalning.

2. *Integration och standarder*

- VMS ska stödja integration med hårdvara från flera leverantörer och vara kompatibelt med ONVIF-standarder.
- Det ska finnas stöd för integration med tredjepartsapplikationer och säkerhetssystem via öppna API:er, t.ex. SOS Alarms larmcentral.

3. *Hantering och användarvänlighet*

- Systemet ska tillhandahålla ett intuitivt och centraliserat gränssnitt för övervakning och hantering av alla videoströmmar, kamerainställningar och användarbehörigheter.
- Funktioner för avancerad sökning i inspelat material, inklusive filtrering efter rörelse, tid, datum och andra parametrar, ska finnas tillgängliga.

4. *Analys och automatisering*

- Systemet ska stödja videoanalys i realtid, exempelvis perimeterövervakning, rörelsedetektering.
- Det ska ha möjlighet att automatisera larm och notifieringar baserat på definierade regler.

5. *Datasäkerhet*

- Videomaterial ska skyddas med kryptering, och åtkomstkontroller för att uppfylla GDPR och NIS2-krav.
- Systemet ska logga all åtkomst och ändringar som görs i plattformen för spårbarhet.

6. *Lagring och redundans*

- Systemet ska stödja både centraliserad och decentraliserad lagring samt redundanslösningar för att minimera risken för dataförlust.
- Edge-lagring ska finnas som backup vid nätverksfel, med möjlighet att synkronisera data till central lagring när anslutningen återställs.

7. *Hybrid- och molnstöd*

- Lösningen ska kunna erbjuda flexibilitet för lagring och åtkomst genom stöd för lokala, molnbaserade och hybridmodeller, baserat på verksamhetens behov.

8. *Flexibilitet för utbyggnad*

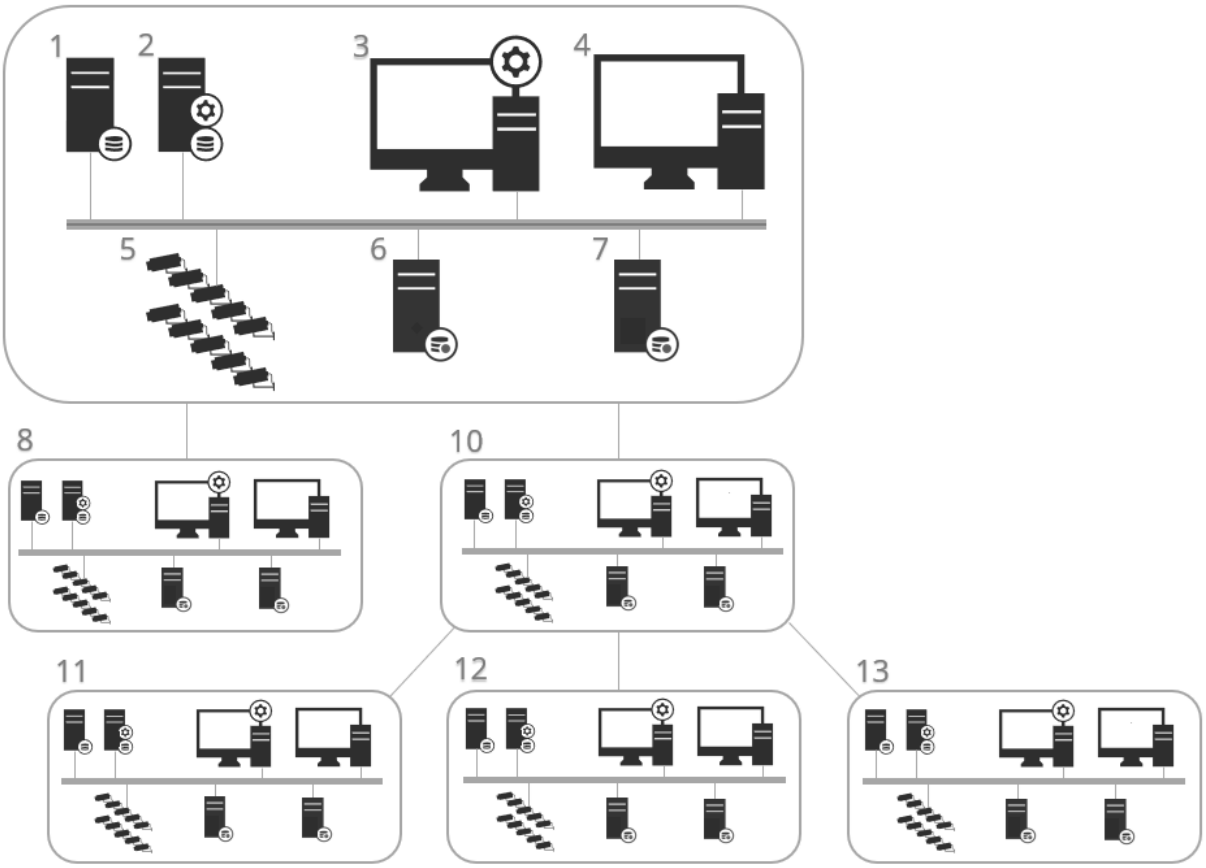
- VMS ska kunna hantera utökningar av kameror, platser och funktioner utan att påverka systemets befintliga prestanda.
- Det ska vara möjligt att integrera nya teknologier och uppdateringar utan omfattande förändringar i systemarkitekturen.

9. *Drift och underhåll*

- Leverantören ska säkerställa att systemet är förberett för regelbundna säkerhetsuppdateringar och underhåll utan driftavbrott.
- Systemet ska ha en support- och övervakningsfunktion som identifierar potentiella problem i realtid.

Exempel federerat system

Ett federerat kamerasystem sammanlänkar flera självständiga övervakningssystem till en central inloggningspunkt. Detta gör det möjligt att övervaka och administrera alla system från en plats, samtidigt som varje enhet behåller sin egen drift och konfiguration.



1. SQL-server
2. Management server
3. Management klient
4. VMS klient
5. Kameror
6. Recording server
7. Failover recording server
8. 8-13 federerade platser

Frågor att fundera på vid investering

Cybersäkerhet och NIS2

- Hur säkerställer ni att ni är skyddat mot moderna cyberhot, inklusive riktade attacker och dataintrång?
- På vilket sätt uppfyller er nuvarande lösning de nya kraven med NIS2 och GDPR, och vad kan förbättras för att säkerställa full efterlevnad?
- Hur hanterar ni säkerhetspatchar och uppdateringar för att minimera sårbarheter i er infrastruktur?

Systemflexibilitet och framtidssäkring

- Hur väl anpassar sig ert nuvarande system till förändrade behov, exempelvis vid utökning av kameror eller integration med andra system?
- Vilka möjligheter har ni idag att enkelt skala upp eller anpassa systemet för nya funktioner som AI-drivna analyser eller IoT-integrationer?
- Har ni funderat på hybridlösningar som kombinerar det bästa av moln- och on-premise-lösningar för både flexibilitet och säkerhet?

Användningsområden

- Vilka nya värden kan ni skapa genom att använda kamerateknologi för verksamhetsoptimering, som kundflödesanalys eller optimering av personalbemanning?
- Hur kan kameror och sensorer bidra till att förebygga incidenter som bränder, vattenläckor eller andra miljörelaterade risker?

Leverantörer och teknik

- Hur ofta utvärderar ni er leverantör och deras förmåga att leverera den senaste teknologin och säkerhetslösningarna?
- På vilket sätt säkerställer ni att er nuvarande leverantör erbjuder bästa möjliga support och uppdateringar för att hålla er lösning aktuell?
- Finns det förbättringar som kan göras för att minska systemets totala kostnad över tid, exempelvis genom lägre energiförbrukning eller smartare lagringslösningar?

Trygghet genom erfarenhet och innovation

På Prudencia Security kombinerar vi vår långa erfarenhet från säkerhets- och fastighetsbranschen med passion för ny teknik och smarta lösningar.

Vi är erfarna projektledare och förstår utmaningarna inom säkerhet och trygghet för fastigheter och verksamheter.

Med expertis och engagemang levererar vi skräddarsydda kameraövervakningssystem och smarta säkerhetslösningar som inte bara möter dagens krav utan också förbereder er för morgondagens möjligheter. Vi brinner för att skapa trygghet genom framtidssäkra lösningar som både ökar säkerhet och effektivitet.

Har du frågor eller vill veta mer om våra tjänster?

Besök vår hemsida på www.prudsec.se eller skicka ett mail direkt till oss på info@prudsec.se.

PRUDENCIA

SECURITY