



MIMIR365
ProperCore

Kommuner · Stat · NIS2 Bilaga I · CRA

NIS2 och CRA för kommuner och statliga myndigheter — OT-compliance för offentlig sektor

Varför offentlig förvaltning är Bilaga I, hur kommunledningens personliga ansvar aktiveras och hur Mimir365 täcker de sex kritiska OT-compliance-gapen.

INNEHÅLL

- 01 NIS2 — klassificering av offentlig förvaltning
- 02 Personligt ledningsansvar — art. 20 i praktiken
- 03 OT-miljön i kommunala byggnader — systemkartan
- 04 CRA och kommunal upphandling från 2027
- 05 De sex NIS2-compliance-gapen
- 06 Checklista: NIS2/CRA-beredskap för offentlig sektor

NIS2

Bilaga I

CRA

Aug 2027

72h

MSB-rapport

6

OT-gap täckta

NIS2 — klassificering av offentlig förvaltning

Offentlig förvaltning är explicit listad i NIS2 Bilaga I (Annex I) som väsentlig sektor. Kommuner, regioner och statliga myndigheter med mer än 50 anställda eller 10 MEUR i omsättning omfattas. I Sverige är MSB (Myndigheten för samhällsskydd och beredskap) tillsynsmyndighet för sektorn.

NIS2-klassificering — offentlig sektor i Sverige

Entitetstyp	NIS2-bilaga	Tillsynsmyndighet	Sanktionsnivå
Statliga myndigheter (>50 anst.)	Bilaga I — Väsentlig	MSB	10 MEUR / 2 % omsättning
Kommuner och regioner (>50 anst.)	Bilaga I — Väsentlig	MSB	10 MEUR / 2 % omsättning
Kommunala bolag — energi, VA, avfall	Bilaga I — Väsentlig	MSB + sektorsmyndighet	10 MEUR / 2 % omsättning
Kommunala bolag — övrigt (>50 anst.)	Bilaga II — Viktig	MSB	7 MEUR / 1,4 % omsättning

Cybersäkerhetslagen och MSB-föreskrifterna

Sverige transponderade NIS2 via Cybersäkerhetslagen (SFS 2024:xxx) som trädde i kraft 2025. MSB:s kompletterande föreskrifter (MSBFS) preciserar de tekniska och organisatoriska kraven. MSB har rätt att genomföra proaktiva tillsynsrevisioner av väsentliga entiteter — inklusive OT-miljön.

NIS2 Artikel 21 — tio obligatoriska åtgärdsdomäner för kommuner

- ! Riskhantering: täcker ALLA system — IT, OT (BMS, HVAC, VA-SCADA) och IoT i kommunala byggnader
- ! Incidenthantering: definierade roller, eskaleringsvägar och 72h-process mot MSB och CERT-SE
- ! Kontinuitetsplanering: BCP/DRP testad — inkluderar OT-haveri (kylbortfall, BMS-kompromiss)
- ! Leverantörskedjans säkerhet: Siemens, Schneider, JCI-åtkomst — avtalad, loggad och tidsbegränsad
- ! Nätverkssäkerhet: OT-segmentering — BMS/HVAC separerat från administrativa IT-system
- ! MFA för all privilegierad åtkomst inklusive BMS och SCADA-system
- ! Sårbarhantering: firmware-CVE:er i BMS-kontroller, HVAC och passerkontroll kartlagda
- ! Kryptografipolicy: data i rörelse och i vila — gäller även OT-kommunikation på fastighetsbus
- ! HR-säkerhet och fysisk säkerhet: tillträde till driftcentraler och OT-managementsystem
- ! Styrelseansvar: kommunstyrelse och nämnder personligen ansvariga — formellt godkänner riskhanteringsplan

&–p Personligt ledningsansvar aktiveras

NIS2 Artikel 20 innebär att kommunstyrelseledamöter, nämnder och generaldirektörer personligen kan hållas ansvariga för NIS2-brott. Kunskapskrav: ledningen ska genomgå regelbunden utbildning i cybersäkerhet och informationssäkerhet. Styrelseledamöter kan, vid upprepade brott, förbjudas att utöva ledningsfunktioner.

Personligt ledningsansvar — art. 20 i praktiken

NIS2 Artikel 20 är en av de mest genomgripande förändringarna för offentlig sektor. Det räcker inte längre att delegera cybersäkerhet till IT-avdelningen — ledningen äger frågan juridiskt och personligt.

Vad Artikel 20 kräver av kommunledningen

- ! Ledningen ska GODKÄNNA riskhanteringsåtgärderna — formellt protokollfört beslut
- ! Ledningen ska ÖVERVAKA genomförandet av NIS2-åtgärder — löpande rapportering
- ! Ledningen ska GENOMGÅ cybersäkerhetsutbildning — dokumenterat och regelbundet
- ! Ledningen är PERSONLIGT ANSVARIG vid brott — ej enbart organisationsansvar
- ! Vid upprepade brott: förbud mot att utöva ledningsfunktioner

Praktiska krav på kommunstyrelsen

Krav	Hur det uppfylls	Dokumentation
Formellt godkännande av riskhanteringsplan	Kommunstyrelsebeslut med NIS2-GAP-analys som beslutsunderlag	Protokoll + GAP-rapport
Löpande övervakning av NIS2-status	Kvartalsvisa lägesrapporter till ledningsgrupp och styrelse	Ledningsprotokoll
Cybersäkerhetsutbildning för ledningen	Strukturerad utbildning — minst 1 gång per år	Utbildningsdokumentation
Leverantörskedja godkänd	Styrelsebeslutat säkerhetskrav i avtal med kritiska leverantörer	Avtal + leverantörsgodkännande

Ø<BÛp Offentlighetsprincipen och sekretess

Kommuners NIS2-dokumentation kan begäras ut under offentlighetsprincipen (OSL).

Säkerhetsklassificerade delar av riskhanteringsplanen — exakt OT-inventering, systemkartor, sårbarhetsinformation — skyddas under 18 kap. OSL (säkerhetsskyddssekretess).

Säkerhetsskyddsklassning av NIS2-dokumentation bör genomföras i samverkan med SÄPO för statliga myndigheter.

OT-miljön i kommunala byggnader — systemkartan

En medelstor kommun med 30–50 fastigheter har typiskt 200–500 nätverksanslutna OT/IoT-enheter som ingen IT-avdelning har inventerat. NIS2 kräver att alla dessa är kartlagda, firmware-versionerade och skyddade.

Sju systemkategorier i kommunala verksamheter

System	Protokoll / plattform	NIS2-risk	Mimir365-åtgärd
BMS / Fastighetsautomation	BACnet/IP, Modbus TCP — Siemens, Schneider, JCI	Obehörig styrning av värme, ventilation, tillträde	OT-inventering, kommandobloggning, anomalidetektion
HVAC / Klimatstyrning	Modbus, LON — Regin, Systemair, Swegon	Set-point-manipulation !' dålig luftkvalitet i skola/vård	Passiv probe, larmkorrelation mot driftparametrar
VA-SCADA (kommunala bolag)	DNP3, Modbus, OPC-UA — Schneider, ABB, GE	Förorening av dricksvatten, översvämning	OT-segmentering, SCADA-loggning, 72h-process
Passerkontroll och CCTV	TCP/IP, OSDP — Axis, Hikvision, ASSA Abloy	Defaultlösenord !' obehörigt tillträde till alla fastigheter	OT-inventering, EOL-flaggning, lösenordspolicy
Trafikstyrning (kommunal)	ITS-protokoll, 4G/LTE — Swarco, Dynniq	Trafikkaos, manipulerade trafiksignaler	OT-probe, segmentering, nätverkslogg
Gatubelysningsstyrning	DALI, 4G-modem — diverse leverantörer	Manipulerat ljussystem, ökad energiförbrukning	IoT-inventering, modem-loggning
Smarta mätare och energi-IoT	DLMS/COSEM, Zigbee — Aidon, Kamstrup	Manipulerade mätvärden !' GDPR och NIS2-brott	IoT-inventering, krypteringskontroll

Det platta nätets farligaste konsekvens

I de flesta kommuner delar BMS-kontroller, HVAC-system och IT-nätet samma VLAN eller ligger på ett delat fastighetsbus utan segmentering. Det innebär att en angripare som komprometterar en BMS-gateway — via ett utnyttjat defaultlösenord eller en gammal firmware-sårbarhet — kan lateralt förflytta sig till kommunens personalregister, ekonomisystem och elevdatabas.

Mimir365 identifierar dessa "nätbryggor" som dag ett-fynd vid OT-inventering.

Segmenteringsrekommendation levereras med konkret nätverksplan — utan att befintlig BMS-konfiguration måste ändras.

CRA och kommunal upphandling från 2027

Cyber Resilience Act (EU 2024/2847) riktar sig mot tillverkare av nätverksanslutna produkter. Men som köpare av OT/IoT-utrustning har kommuner ett indirekt ansvar — och från augusti 2027 är CRA-certifikat en förutsättning för CE-märkning.

CRA-krav på produkter kommuner upphandlar

CRA-klass	Typiska kommunala produkter	Krav på tillverkaren
Default	Temperaturgivare, luftkvalitetssensorer, enklare IoT-noder, gatubelysningsmoduler	Självdeklaration — utökat CE-märke
Klass I	BMS-accesspunkter, passerkontroll-servrar, smarta mätare, digitala lås	Tredjepartsgranskning eller harmoniserad standard (EN IEC 62443)
Klass II	Core switches, brandväggar, SCADA-kommunikationsmoduler	Obligatorisk tredjeparts-certifiering
IACS-komponenter	Avancerade PLC:er och RTU:er i VA-SCADA och trafikstyrning	EU-certifiering — strängaste klassen

Kommuners upphandlingsansvar under CRA

- ! Från aug 2027: allt nytt nätverksanslutet OT/IoT-equipment kräver CRA-certifikat för att CE-märkas
- ! Kommunala ramavtal (SKR-avtal) innehåller idag inga CRA-krav — uppdatering krävs
- ! Upphandlare: lägg till cybersäkerhetskrav och CRA-roadmap-krav i alla LOU-upphandlingar nu
- ! Existerande installationer: CRA täcker ej retroaktivt — men NIS2 kräver riskhantering ändå
- ! Säkerhetspatch-krav: CRA kräver tillverkaren tillhandahåller uppdateringar — ej en engångsprodukt
- ! SBOM (Software Bill of Materials): CRA-certifierade produkter levereras med dokumenterad komponentlista

Ø=ÞØ Strategisk upphandlingspunkt

En typisk kommunupphandling av fastighetsdrift 2024–2026 binder kommunen till en leverantörs BMS-plattform i 7–10 år. Utan CRA-krav i förfrågningsunderlaget riskerar kommunen att 2027 ha en ny installation fylld av icke-certifierade enheter och ingen garanterad patch-försörjning. Mimir365 levererar ett upphandlingsstöd med cybersäkerhetskrav anpassat för LOU och SKR-ramavtal.

De sex NIS2-compliance-gapen

Dessa sex gap är de vanligaste bristerna vi identifierar vid NIS2-kartläggning av kommuner och statliga myndigheter. Varje gap är ett potentiellt brott mot NIS2 och ett dokumenterat säkerhetshål.

Gap 1 — Ingen OT-inventering av kommunala byggnader

NIS2 Artikel 21 kräver fullständig kartläggning av alla OT/IoT-system. En medelstor kommun har 200–500 nätverksanslutna BMS-noder, sensorer och passerkontrollers fördelade över skolor, bibliotek och förvaltningsbyggnader — och ingen komplett lista.

Mimir365-lösning: Passiv OT-inventering via nätverksprobe identifierar alla enheter, firmware-versioner, kommunikationsprotokoll och leverantörskopplingar utan att störa drift eller validerade system. Komplet CMDB levereras från dag ett.

Gap 2 — Leverantörers åtkomst till BMS är okontrollerad

Siemens, Schneider Electric och Johnson Controls har permanenta VPN-åtkomster för fjärrövervakning och service av BMS-system. Dessa är typiskt inte loggade, inte tidsbegränsade och aldrig reviderade. En komprometterad leverantörsklient = obehörig kontroll av värme, ventilation och tillträde i alla kommunens fastigheter.

Mimir365-lösning: All OT-nätverkstrafik per leverantör loggas automatiskt. Leverantörsåtkomster identifieras, dokumenteras och kan tidsbegränsas. Leverantörsrevisionsrapport genereras löpande — NIS2 art. 21.2(d) uppfyllt.

Gap 3 — OT och IT på platt nät

BMS-kontroller och HVAC-system delar i de flesta kommuner VLAN eller nätverkssegment med administrativa IT-system. En angripare som via en IoT-sensor eller BMS-gateway tar sig in kan lateralt förflytta sig till kommunens personalregister, ekonomisystem och skolplattformar. Det är ett kombinerat NIS2- och GDPR-brott.

Mimir365-lösning: OT-inventering identifierar nätbryggor och "flat network"-zoner. Segmenteringsrekommendation levereras med konkret nätverksplan. Implementering sker på nätverksnivå utan ändringar i BMS-konfiguration.

Gap 4 — Personligt ledningsansvar ej dokumenterat

Kommunstyrelseledamöter och nämnder är juridiskt ansvariga för NIS2-efterlevnad (art. 20) men saknar ofta formellt beslutsunderlag om riskhanteringsåtgärder. Utan protokollfört beslut och dokumenterad utbildning är personligt ansvar aktivt men skyddet mot det saknas.

Mimir365-lösning: Riskhanteringsrapport med OT-GAP-analys levereras i format anpassat för kommunstyrelsebeslutsunderlag. Kvartalsvisa NIS2-statusrapporter för löpande övervakning. Utbildningsmaterial för kommunledning ingår.

Gap 5 — CRA-krav saknas i upphandlingsunderlag

Befintliga ramavtal och LOU-upphandlingar av teknisk utrustning innehåller inga cybersäkerhetskrav och inga CRA-krav. Upphandlingar genomförda 2024–2026 kan binda kommunen till CRA-icke-kompatibel utrustning långt in på 2030-talet.

Mimir365-lösning: CRA-klassning av befintlig OT-park plus upphandlingsstöd med cybersäkerhetskrav anpassat för LOU och SKR-ramavtal. Leverantörers CRA-roadmap begärs in och utvärderas som del av upphandlingsprocess.

Gap 6 — Ingen 72h-incidentprocess för OT

NIS2 kräver tidig varning till CERT-SE inom 24h och fullständig rapport till MSB inom 72h med rekonstruerad händelsetidslinje. Kommuner saknar OT-nätverkslogg. Vid ett BMS-intrång eller VA-SCADA-kompromiss kan kommunen inte rekonstruera vad som hände — och riskerar formell tillsyn för ofullständig rapportering.

Mimir365-lösning: Kontinuerlig OT-nätverksloggning med 12 månaders retention. Korrelation mot IT-SIEM och fysisk tillträdeslogg. MSB-rapportmall med OT-händelsetidslinje genereras automatiskt vid säkerhetshändelse.

Checklista: NIS2/CRA-beredskap för offentlig sektor

Använd denna lista för att kartlägga er nuvarande NIS2-status. Mimir365 automatiserar samtliga tekniska punkter löpande — de organisatoriska punkterna kräver kommunens egna beslut.

Governance och ledningsansvar (art. 20)

- ☐ Utsedd säkerhetsansvarig (CISO eller motsv.) med OT-mandat
- ☐ Kommunstyrelse/GD formellt godkänt riskhanteringsplan — protokollfört
- ☐ Löpande cybersäkerhetsutbildning för ledningen dokumenterad
- ☐ NIS2-status rapporteras kvartalsvisa till kommunstyrelse/ledning
- ☐ MSB-kontakt etablerad — ansvarig tjänsteperson utsedd

OT/IoT-inventering och segmentering

- ☐ Komplet list över BMS-noder, HVAC, passerkontroll och IoT i alla fastigheter
- ☐ Firmware-versioner kartlagda med CVE-exponering dokumenterad
- ☐ OT-nät separerat från IT-nät (BMS-VLAN isolerat)
- ☐ VA-SCADA och trafikstyrning cybersäkerhetsgranskat
- ☐ Defaultlösenord bytta på alla OT- och IoT-enheter
- ☐ Leverantörens fjärråtkomst loggad, avtalad och tidsbegränsad

CRA-upphandlingsförberedelse

- ☐ CRA-klassning genomförd för befintlig OT/IoT-park
- ☐ Upphandlingsmallar uppdaterade med cybersäkerhetskrav
- ☐ Leverantörens CRA-roadmap begärd för Klass I och II-utrustning
- ☐ SKR-ramavtal granskade mot CRA-krav

Incidenthantering och 72h-process

- ☐ 72h-incidentprocess dokumenterad och testad för OT-incident
- ☐ OT-nätverkslogg aktiv med minst 12 månaders retention
- ☐ OT-logg korrelerad mot IT-SIEM och fysisk tillträdeslogg
- ☐ MSB-rapportmall klar med OT-tidslinje
- ☐ Kontinuitetsplan (BCP) inkluderar OT-haveri (BMS-kompromiss, VA-SCADA)
- ☐ CERT-SE tidig varning (<24h) — kontaktvägar testade

Redo att ta nästa steg?

Boka ett kostnadsfritt strategisamtal med en av våra specialister.

mimir365.se/kontakt

security@mimir365.se · privacy@mimir365.se · legal@mimir365.se

© 2026 Mimir365 AB · Org. nr 556610-3205 · c/o HighFive · Trade Center, våning 2 & 3 · Kristian IV:s väg 3 · 302 50 Halmstad

Innehållet i denna guide är informativt och utgör inte juridisk rådgivning. Mimir365 AB ansvarar inte för beslut fattade på grundval av guidens innehåll.