MIMIR365
ProperCore

Datacenter · NIS2 Bilaga I · CRA

NIS2 och CRA för datacenter — OT-attackyta, klassning och compliance-gap

Varför datacenteroperatörer är Bilaga I i NIS2, hur CRA påverkar er utrustning och hur Mimir365 täcker de sex kritiska OT-compliance-gapen.

INNEHÅLL

NIS2	CRA	72h	6
Bilaga I	Aug 2027	PTS-rapport	OT-gap täckta

Mimir365 AB · mimir365.se · Utgiven maj 2026 · 24 sidor

NIS2 — klassificering och Bilaga I-krav

Datacenteroperatörer är explicit listade i NIS2 Bilaga I (Annex I) under sektorn "Digital infrastruktur". Det innebär den strängaste tillsynsregimen — proaktiva revisioner av PTS, personligt ledningsansvar och sanktioner utan storlekströskel.

Tre driftsformer — NIS2-klassning

Driftsform	NIS2-bilaga	Sanktionsnivå	Tillsynsmyndighet
Co-location, hyperscale, enterprise-DC	Bilaga I — Väsentlig	10 MEUR / 2 % omsättning	PTS (Post- och telestyrelsen)
IaaS/PaaS/SaaS-leverantörer, MSP	Bilaga I — Väsentlig	10 MEUR / 2 % omsättning	PTS + IMY vid personuppgifter
Privata serverrum, edge-DC i NIS2-org.	Bilaga II — Viktig	7 MEUR / 1,4 % omsättning	PTS / sektorsmyndighet

Ingen storlekströskel för datacenteroperatörer

Till skillnad från de flesta NIS2-sektorer gäller storleksgränserna ("e50 anst. / "e10 MEUR) INTE för datacenteroperatörer listade i Annex I. Är ni datacenteroperatör omfattas ni oavsett storlek.

NIS2 Artikel 21 — tio obligatoriska åtgärdsdomäner

- !’ Riskhantering: täcker ALLA system — IT OCH OT (kraft, kyla, BMS, passerkontroll)
- !’ Incidenthantering: definierade roller, eskaleringsvägar och 72h-process mot PTS
- !’ Kontinuitetsplanering: BCP/DRP testad — inkluderar OT-haveri (kylbortfall, UPS-fel)
- !’ Leverantörskedjans säkerhet: Schneider, Vertiv, Stulz fjärråtkomst — avtalad och loggad
- !’ Nätverkssäkerhet: OT-segmentering — kraft/kyla/BMS separerat från IT och kund-VLAN
- !’ MFA för all privilegierad åtkomst inklusive OT-management-system
- !’ Sårbarhantering: firmware-CVE:er i UPS/PDU/CRAC kartlagda och patchade
- !’ Kryptografipolicy: data i rörelse och i vila — gäller även OT-kommunikation
- !’ HR-säkerhet och fysisk säkerhet: tillträde till maskinsalen och OT-system
- !’ Styrelseansvar: ledningen personligen ansvarig, formellt godkänner riskhanteringsplanen

&¡ Personligt ledningsansvar

NIS2 Artikel 20 innebär att ledningen personligen kan hållas ansvarig för NIS2-brott. Styrelseledamöter kan förbjudas att utöva ledningsfunktioner. Kunskapskrav: ledningen ska genomgå regelbunden utbildning i cybersäkerhet.

CRA och datacenter-OT

Cyber Resilience Act (EU 2024/2847) är en produktförordning som träder i kraft i faser till augusti 2027. Den styr tillverkarna av er DC-utrustning — men som operatör bär ni ansvar för att hålla CRA-certifierade produkter säkra och patchade.

CRA-klassning av typisk datacenter-OT

CRA-klass	Utrustning i datacenter	Krav på tillverkaren
Default	PDU, miljösensorer (temperatur/fukt/läcka), enskilda IoT-enheter	Självdeklaration — CE-märke utökat
Klass I	UPS med SNMP/web-hantering (APC, Eaton, Vertiv), passerkontroll-servrar, KVM-switchar	Tredjepartsgranskning eller harmoniserad standard
Klass II	Core switches, routrar, brandväggar (Cisco, Arista, Palo Alto, Fortinet, Check Point)	Obligatorisk tredjepartscertifiering
IACS-komponenter	BMS-kontroller (Siemens Desigo CC, Schneider EcoStruxure), brandlarm-PLC, ATS-kontroller	EU-certifiering — strängaste klassen

Dubbelt ansvar: NIS2 för befintlig utrustning, CRA för ny

- !’ CRA gäller INTE retroaktivt — befintlig utrustning täcks inte automatiskt
- !’ NIS2 kräver ändå riskhantering för befintlig utrustning — CVE:er i APC-firmware är ett NIS2-problem nu
- !’ Inköp efter aug 2027: allt nytt nätverksanslutet OT-equipment kräver CRA-certifikat
- !’ Operatörens ansvar: security patches från tillverkaren ska installeras inom rimlig tid
- !’ Klass II (nätverksutrustning): obligatorisk tredjepartscertifiering — börja begär CRA-roadmap av leverantörer nu

Ø=Ý Strategisk nyckelpunkt

En DC-operatör med 200 enheter OT-utrustning har typiskt 15–25 tillverkare med åldersspann 3–15 år. Ingen gemensam säkerhetsarkitektur. CRA-compliance på pappret löser ingenting om ni inte vet vad som faktiskt är uppkopplat och vilket firmware det kör. Mimir365 är det operativa lagret som gör att ni faktiskt kan efterleva båda direktiven.

OT/IoT-attackytan i maskinsalen

Moderna datacenter har välskyddad IT-miljö — brandväggar, SIEM, SOC, penetrationstestning. Men ett parallellt OT-nät av kraft-, kyl- och fastighetssystem saknar i stort sett all cybersäkerhetskontroll.

Sju systemkategorier som NIS2 kräver att ni kontrollerar

System	Typ / protokoll	Attackscenario	Mimir365-åtgärd
Strömförsörjning (UPS/ PDU/ATS)	SNMP v1/v2, webgränssnitt — APC, Eaton, Vertiv	Fjärrstyrd strömavstängning för hela rack-rader	OT-inventering, firmware CVE-scan, SNMP-segmentering
Kylsystem (CRAC/ CRAH/Chiller)	Modbus TCP, webgränssnitt — Vertiv, Stulz, Schneider	Set-point-höjning !’ termisk haveri 15–45 min	OT-probe, anomalidetektion, set-point-larm
BMS / SCADA	BACnet/IP, Modbus TCP — Siemens Desigo, EcoStruxure	Styr kyla, tillträde och brand utan autentisering	BMS-probe, kommandobloggning, korrelation IT-SIEM
Passerkontroll och CCTV	TCP/IP — Lenel, Software House, Axis, Hikvision	EOL Windows, defaultlösenord !’ fysiskt tillträde	OT-inventering, EOL-flaggning, loggkorrelation
Out-of-band management	IPMI/BMC, konsolservrar — Opengear, Lantronix	Brygga OT–IT, lateral förflyttning	Management VLAN-isolering, loggning
Brandskydd och suppression	BACnet, proprietärt — Siemens, Honeywell	Obehörigt utlöst FM-200 !’ IT-haveri och personrisk	BMS-loggning, anomalidetektion på suppression-kommandon
Miljöövervakning (IoT)	MQTT mot leverantörens moln — diverse tillverkare	Sensorspoofing, okontrollerad dataöverföring	Proxy-loggning, segmentering mot externa moln

Termisk attack — snabbaste vägen till totalt driftstopp

En angripare med åtkomst till ett CRAC/CRAH-system höjer set-point-temperaturen med 8–10°C. Vid full serverbelastning (typiskt i ett modernt DC) stiger temperaturen i drabbade rack från 22°C till över 40°C på 15–45 minuter.

Servrar börjar CPU-throttling, sedan emergency shutdown. Utan OT-nätverkslogg kan operatören inte avgöra om det är tekniskt fel eller riktad attack — och saknar underlag för NIS2:s obligatoriska 72h-rapport till PTS.

De sex NIS2/CRA-compliance-gapen

Dessa sex gap är de vanligaste bristerna vi identifierar vid kartläggning av en datacenter-anläggnings NIS2-beredskap. Varje gap är ett potentiellt NIS2-brott och en dokumenterad attackyta.

Gap 1 — UPS och PDU utan cybersäkerhet

APC/Vertiv UPS-system kör SNMP v1/v2 med okrypterade community-strängar ("public"/"private") och web-gränssnitt med defaultlösenord. Ofta på samma VLAN som IT-management. En komprometterad UPS-controller = fjärrstyrd strömavstängning.

Mimir365-lösning: Passiv OT-inventering kartlägger alla UPS/PDU-enheter med firmware-version och SNMP-konfiguration. CVE-scan identifierar kända sårbarheter. OT-nätverkssegmentering isolerar kraft-VLAN.

Gap 2 — BMS är okartlagd attackyta

Siemens Desigo och Schneider EcoStruxure BMS kör BACnet/IP och Modbus TCP utan autentisering som standard. BMS styr kyla, tillträde och brandskydd. En BMS-kompromiss kan orsaka termisk haveri, obehörigt fysiskt tillträde och felaktigt utlöst brandskydd.

Mimir365-lösning: OT-probe på BMS-nätverkssegmentet loggar alla BACnet/Modbus-kommandon. Anomalidetektion larmar vid set-point-ändringar utanför operativa parametrar. Händelselogg korreleras med IT-SIEM.

Gap 3 — Leverantörsåtkomst okontrollerad

Schneider Electric, Vertiv och Stulz har permanenta VPN-tunnlar för fjärrövervakning och service. Dessa är typiskt inte loggade, inte tidsbegränsade och aldrig reviderade. NIS2 Artikel 21.2(d) kräver att leverantörers åtkomst är avtalad, loggad och kontrollerad.

Mimir365-lösning: All OT-nätverkstrafik per leverantör och enhet loggas automatiskt. Åtkomst kan tidsbegränsas via nätverkspolicyer. Leverantörsrevisionsrapport genereras löpande för NIS2-dokumentation.

Gap 4 — Firmware-desert i kraft och kyla

UPS- och CRAC-firmware är typiskt 3–7 år bakom aktuell version. CVE-2021-22805 (Schneider APC), CVE-2022-29953 (Vertiv Liebert) och liknande kritiska sårbarheter är publikt dokumenterade sedan år — men aldrig patchade i fält.

Mimir365-lösning: Kontinuerlig kartläggning av OT-firmware mot NVD/CVE-databaser. Automatisk advisory-varning när ny sårbarhet publiceras för er specifika utrustningsprofil. Patchningsplan med prioritering.

Gap 5 — Fysisk säkerhet är cybersäkerhet

Access-kontroll-servrar kör Windows Server 2016–2019 med utgående support. CCTV-kameror (Hikvision, Axis) med defaultlösenord. Access control-systemets databas har sällan MFA. Kompromiss = obevakat fysiskt tillträde till all hårdvara i maskinsalen.

Mimir365-lösning: Passerkontroll och CCTV ingår i OT-inventeringen. Flaggar EOL-OS och defaultkonfigurationer. Loggkorrelation: fysisk tillträdeshändelse mot IT-säkerhetslogg och OT-nätverkslogg.

Gap 6 — Ingen OT-incidentlogg

NIS2 kräver 72h-rapport till PTS med rekonstruerad händelsekedja. Datacenter har IT-SIEM men noll OT-logg. Vid termisk attack, UPS-manipulation eller BMS-intrång saknas underlag. En ofullständig rapport kan utlösa formell tillsyn.

Mimir365-lösning: Kontinuerlig OT-nätverksloggning med 12 månaders retention. Korrelation mot IT-SIEM och fysisk tillträdeslogg. MSB/PTS-rapportmall med rekonstruerad OT-tidslinje genereras automatiskt.

Redundans, kontinuitet och incidenthantering

NIS2 kräver dokumenterad redundans, testad kontinuitetsplan och fungerande 72h-incidentprocess. Uptime Institutes TIER-klassning ger ramverket för redundanskraven.

TIER-klassning och NIS2-relevans

TIER	Tillgänglighet	Redundans	NIS2-relevans
I	99.671 %	Ingen	Ej lämplig för NIS2-skyldiga — enstaka fel ger driftstopp
II	99.741 %	Delvis N+1	Marginal — planerat underhåll kräver partiellt driftsstopp
III	99.982 %	N+1 concurrent maintainable	Miniminivå för de flesta NIS2 Bilaga I-entiteter
IV	99.995 %	2N+1 fault tolerant	Rekommenderat för samhällskritiska datacenter

NIS2-incidentrapporteringskedjan — datacenter

Tid	Åtgärd	Mottagare
0–4 h	Initial bedömning och inneslutning — OT och IT	Intern CSIRT/SOC
4–24 h	Tidig varning (early warning) — inklusive OT-incident	NCSC / CERT-SE
24–72 h	Fullständig incidentrapport med OT-tidslinje	PTS (datordrift) + MSB
1 månad	Slutrapport med root cause och åtgärdsplan	PTS + intern ledning

BCP/DRP — OT-perspektivet

- Kylbortfall: dokumenterat RTO — hur lång tid tills termisk shutdown vid total CRAC-förlust?
- Strömavbrott: UPS-autonomi × dieselgeneratorns starttid — gap dokumenterat och testat
- BMS-kompromiss: fallback-läge för manuell kylstyrning definierat och övat
- Leverantörsberoende: eskalationsvägar till Schneider/Vertiv/Stulz vid OT-incident
- Kommunikationsplan: kunder informeras vid incident som påverkar SLA

Checklista: NIS2/CRA-beredskap datacenter

Använd denna lista för att kartlägga er nuvarande NIS2-status och identifiera de mest kritiska gapen. Mimir365 automatiserar samtliga punkter löpande.

NIS2 Governance och ledningsansvar

- [ ] Utsedd CISO eller säkerhetsansvarig med OT-mandat
- [ ] Styrelsen formellt godkänt riskhanteringsprocessen
- [ ] Riskhantering dokumenterad för OT (kraft, kyla, BMS, passerkontroll)
- [ ] Leverantörskedjans säkerhet kartlagd och avtalad (Schneider, Vertiv m.fl.)
- [ ] Kontakt med PTS etablerad och dokumenterad

OT/IoT-inventering och segmentering

- [ ] Komplett lista över UPS, PDU, CRAC/CRAH, BMS-noder och IoT-enheter
- [ ] Firmware-versioner kartlagda med CVE-exponering
- [ ] OT-nät separerat från IT-nät och kund-VLAN
- [ ] SNMP v1/v2 ersatt med v3 eller OT-nätverksisolering
- [ ] Defaultlösenord bytta på alla OT-enheter
- [ ] Leverantörers fjärråtkomst loggad och tidsbegränsad

CRA-förberedelse

- [ ] CRA-klassning genomförd för alla nätverksanslutna OT-enheter
- [ ] Leverantörers CRA-roadmap begärd för Klass I och II-utrustning
- [ ] Inköpsprocess uppdaterad: CRA-krav gäller från aug 2027
- [ ] Patch-hanteringsprocess för OT-firmware dokumenterad

Incidenthantering och 72h-process

- [ ] 72h-incidentprocess dokumenterad och testad specifikt för OT-incident
- [ ] OT-nätverkslogg aktiv med minst 12 månaders retention
- [ ] OT-logg korrelerad mot IT-SIEM och fysisk tillträdeslogg
- [ ] MSB/PTS-rapportmall klar med OT-tidslinje
- [ ] Kontinuitetsplan (BCP) inkluderar OT-haveri (kylbortfall, UPS-fel)

Energi och ESG-rapportering

- [ ] PUE mäts och rapporteras kontinuerligt (EED-krav för DC >1 MW)
- [ ] WUE och CUE spåras för CSRD-rapportering
- [ ] Energioptimering dokumenterad: ASHRAE A2-set-points, frikyla
- [ ] Förnybar energiandel (REF) rapporteras mot EU-taxonomin

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