MIMIR365
ProperCore

Laboratorium · NIS2 · CRA · ISO 17025

NIS2 och CRA för laboratorier — OT-inventering, compliance och kalibreringsintegritet

Varför labbet OT-system faller under NIS2, hur CRA påverkar er instrumentpark och hur Mimir365 täcker de sex kritiska compliance-gapen.

INNEHÅLL

NIS2	CRA	72h	6
Bilaga I & II	Aug 2027	Incidentrapport	OT-gap täckta

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

NIS2 — vilket labb klassas och varför

NIS2 (EU 2022/2555) expanderar scope kraftigt jämfört med NIS1. Laboratorier faller under direktivet via tre olika bilagevägar beroende på verksamhetstyp — klassificeringen avgör tillsynsregim och sanktionsnivå.

Klassificering per labbtyp

Labbtyp	NIS2-bilaga	Entitetsnivå	Grund
Kliniska laboratorier	Bilaga I — Hälsa	Väsentlig	Kritisk hälsoinfrastruktur — direkt tillsyn
Pharma-produktionslab	Bilaga II — Tillverkning	Viktig	Medicinteknisk tillverkning
Forskningslab (RISE, uni)	Bilaga II — Forskning	Viktig	Explicit i NIS2 Annex II sedan 2022
Livsmedels- och miljölab	Bilaga II — Livsmedel	Viktig	Livsmedelssäkerhetskedjan
ISO 17025-testlab	Bilaga II — Tillverkning	Viktig	Beroende på primär kundsektor

Storlekströskel och undantag

Medelstora ("e50 anställda eller "e10 MEUR omsättning) och stora företag omfattas. Mikro- och småföretag undantas om de inte är kritiska oberoende av storlek — exempelvis om de är enda leverantör av en samhällskritisk funktion.

NIS2 Artikel 21 — tio obligatoriska åtgärdsdomäner

- !’ Riskhanteringsprocess som täcker ALLA system — inklusive OT och IoT
- !’ Incidenthantering med definierade roller och eskaleringsvägar
- !’ Kontinuitetsplanering: BCP måste täcka LIMS-haveri och BMS-kompromiss
- !’ Leverantörskedjans säkerhet: instrumentleverantörers fjärråtkomst ska vara avtalad och loggad
- !’ Nätverkssäkerhet och segmentering: OT-nät separerat från IT
- !’ MFA för all fjärråtkomst till OT-system
- !’ Kryptografi: kryptografipolicy för data i rörelse och i vila
- !’ HR-säkerhet och fysisk säkerhet
- !’ Sårbarhantering och patch-hantering för OT-firmware
- !’ Styrelseansvar: ledningen ska godkänna och ansvara för säkerhetsåtgärderna

& Det kritiska misstaget

De flesta labb tänker "IT-säkerhet" när NIS2 nämns — och missar 80 % av attackytan. Det är OT-systemen (instrumentbussen, BMS, IoT-gateways) som NIS2 specifikt kräver att ni inventerar, segmenterar och dokumenterar. Har ni ingen komplett inventering av nätverksanslutna instrument idag är ni redan i otakt med Artikel 21.

CRA — hur EU:s produktlag påverkar er utrustning

Cyber Resilience Act (EU 2024/2847) är en produktförordning som träder i kraft i faser till augusti 2027. Den styr tillverkarna av er labbutrustning — men som operatör har ni skyldigheter som följer med.

CRA-klassning av typisk lab-OT

Klass	Typiska instrument i labb	Krav på tillverkaren
Default	HPLC, GC-MS, spektrofotometrar, IoT-sensorer	Självdeklaration — CE-märke utökat
Klass I	Nätverkshanterbar UPS, access-controllers i reglerade utrymmen	Tredjepartsgranskning eller harmoniserad standard
Klass II	Industri-PLC, brandväggsutrustning, HSM	Obligatorisk tredjepartscertifiering
IACS-komp.	Bioreaktorkontroll, autoklav-PLC, cleanroom-styrning	EU-certifiering — strängaste klass

Vad CRA innebär för labb som operatör

- !’ Inköp efter aug 2027: allt nytt instrument måste vara CRA-certifierat — CE-märket utökas
- !’ Befintlig utrustning: CRA täcker inte retroaktivt, men NIS2 kräver ändå riskhantering
- !’ Säkerhetsuppdateringar: ni måste ta emot och installera tillverkarens security patches
- !’ En HPLC med Windows XP-styrdator är ett NIS2-problem oavsett CRA-status
- !’ Vulnerability disclosure: aktivt utnyttjade sårbarheter ska rapporteras till ENISA

Ø=Ý Nyckelpunkten

NIS2 säger "du ansvarar för säkerheten i dina OT-system" och CRA säger "tillverkaren ska leverera säkra produkter." Men i ett typiskt labb finns instrument från 7–15 tillverkare med åldersspann 2–20 år och ingen gemensam säkerhetsarkitektur. Mimir365 är det operativa lagret som gör att ni faktiskt kan efterleva båda.

Lab-OT och IoT — den faktiska systemkartan

Ett medelstort ISO 17025-ackrediterat labb har typiskt sju OT/IoT-systemkategorier. Alla är potentiella NIS2-skyldigheter — de flesta är i dag okartlagda.

Sju systemkategorier som NIS2 kräver att ni kontrollerar

System	Protokoll	NIS2-risk	Mimir365-åtgärd
Analytiska instrument (HPLC, GC-MS)	Empower / OpenLAB, Ethernet	Manipulerade analysresultat	Passiv discovery, OT-logg
LIMS-infrastruktur	OPC-UA, REST, proprietärt	IP-stöld, datamanipulation	Nätverkssegmentering
Cleanroom BMS (PLC/ SCADA)	Modbus, BACnet, Profibus	Set-point-manipulation, ISO 14644-brott	OT-probe, anomalidetektion
Miljöövervakning (IoT)	MQTT mot tillverkarens moln	Okontrollerad dataöverföring	Proxy-loggning, segmentering
Processtyrsystem (autoklave)	RS-485, TCP/IP	GxP-validerat — specialhantering	Nätverksnivå, ej applikation
Kalibreringsinfrastruktur	Egna databaser, RISE/ NIST	Manipulerade data — förlorad ackr.	Hash-kedja, audit trail
Fastighetssystem (HVAC, gas)	BACnet, KNX, proprietärt	Avbrottssabotage, fysisk säkerhet	BMS-inventering, loggning

Den kritiska risken: manipulerade kalibreringsdata

En angripare med åtkomst till instrumentnätet kan ändra kalibreringsdata utan att trigga ett IT-larm. Resultatet: analyser ger felaktiga svar i dagar eller veckor. För ett kliniskt labb innebär det direkt patientrisk. För ett ISO 17025-ackrediterat labb innebär det återkallad ackreditering.

Mimir365 skriver kalibreringsloggar till ett oföränderligt audit trail med hash-kedja. Varje post är kryptografiskt verifierbar — SWEDAC och kunder kan verifiera att ingen post modifierats.

De sex compliance-gapen NIS2 blottar

Dessa sex gap är de vanligaste bristerna vi hittar när vi kartlägger ett labs NIS2-beredskap. Varje gap är ett potentiellt NIS2-brott och en attackyta.

Gap 1 — Ingen vet vad som finns

NIS2 kräver komplett inventering. De flesta labb saknar en lista över nätverksanslutna instrument, firmware-versioner och vilka leverantörer som har fjärråtkomst.

Mimir365-lösning: Passiv nätverksdiscovery bygger automatiskt CMDB med enhet, fabrikat, firmware, IP/MAC och leverantörskoppling — utan att störa validerade system.

Gap 2 — Leverantörsåtkomst okontrollerad

Agilent, Waters, Roche, Sartorius har VPN-klienter och supportkontoåtkomst till era instrument. NIS2 art. 21.2(d) kräver att detta är kartlagt, avtalat och loggat. De flesta labb har idag ingen kontroll.

Mimir365-lösning: Automatisk loggning av all OT-nätverkstrafik per leverantör och instrument. Åtkomstloggen för leverantörsrevisioner genereras löpande.

Gap 3 — BMS är OT utan cybersäkerhet

Cleanroom-PLC:erna kör Modbus/BACnet utan autentisering. En angripare kan ändra differenstryck eller temperaturset-points utan att trigga ett larm. Det är en NIS2-risk och en ISO 14644-risk.

Mimir365-lösning: OT-probe på BMS-segmentet loggar alla kommandon, detekterar anomalier och kopplar BMS-händelser direkt till ISO 14644-compliance-loggen.

Gap 4 — IoT-gateways utan insyn

Miljöövervakningens IoT-enheter synkroniserar direkt mot tillverkarens moln via MQTT utan att labbet ser trafiken. Det är per definition en CRA-relevant attackyta och ett NIS2-kompliansbrott (okontrollerad dataöverföring).

Mimir365-lösning: OT-nätverkssegmentering bryter direktanslutningen. All datatrafik routas via loggad proxy — molnsynken fungerar men med fullständig insyn och loggning.

Gap 5 — Kalibreringsdata inte skyddad

Kalibreringsdata i ett ISO 17025-ackrediterat labb är business-critical, inte IT-kritisk. En manipulerad kalibrerings-post kan leda till återkallad ackreditering eller — i klinisk kontext — direkt patientskada.

Mimir365-lösning: Oföränderligt audit trail med hash-kedja. Varje kalibrerings-post är kryptografiskt verifierbar — SWEDAC och kunder kan verifiera att ingen post modifierats.

Gap 6 — Ingen 72-timmarsprocess

NIS2 art. 23 kräver tidiga varningar till CSIRT inom 24 timmar och fullständig incidentrapport till MSB inom 72 timmar. Utan OT-loggning kan labbet inte rekonstruera vad som hände, när och på vilka system.

Mimir365-lösning: 12 månaders OT-nätverkslogg korrelerad mot LIMS-events och BMS-larm. Tidslinjerapport i MSB:s rapportformat genereras automatiskt.

Kalibreringsintegritet och ISO 17025-synergi

ISO 17025 och NIS2 är komplementära — inte konkurrerande. Ackrediteringssystemet kräver redan dokumenterade processer, oföränderliga loggar och strukturerad avvikelsehantering. Mimir365 adderar NIS2-dimensionen ovanpå befintlig kvalitetskultur.

Vad ska loggas per instrument för att uppfylla båda

- Unikt instrument-ID, fabrikat, modell, serienummer och firmware-version
- Nätverksanslutning: IP/MAC, port, protokoll (ISO 17025 + NIS2 inventering)
- Senaste kalibreringsdatum, certifikat-nummer, spårbarhet till SI
- Nästa kalibreringsförfallodatum med automatisk påminnelse 30 dagar
- Mätosäkerhet och tillåten avvikelse (spec-gräns) — kalibrerat mot GUM
- Leverantörsberoenden: vem har fjärråtkomst och när — kryptografisk logg
- Historik: korrigeringsåtgärder, utbyten, firmware-uppdateringar

GxP-säker implementation

Det viktigaste för pharma- och kliniska labb: Mimir365 arbetar på nätverksnivå, inte applikationsnivå. Validerade GxP-system rörs aldrig. Ingen re-validering krävs. Compliance-lagret adderas utan att rubba det validerade IT-systemet.

Ø>Ý Säljcykelns fördel

ISO 17025-ackrediterade labb förstår compliance — de lever i det. NIS2 adresserar en ny dimension av samma infrastruktur. Säljcykeln är kortare eftersom kunden redan har compliance-kulturen. Mimir365 behöver bara visa att OT är det gap som fattas.

Checklista: NIS2/CRA-beredskap för labb

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

NIS2 Klassificering och governance

- [ ] Er klassificering fastställd: Bilaga I (Väsentlig) eller Bilaga II (Viktig)?
- [ ] Styrelsen informerad om NIS2-krav och ledningsansvar
- [ ] Riskhanteringsprocess dokumenterad som täcker OT och IoT
- [ ] CISO eller säkerhetsansvarig utsedd med mandat över OT

OT/IoT-inventering

- [ ] Fullständig lista över nätverksanslutna instrument med firmware-status
- [ ] Alla OT-leverantörers fjärråtkomst kartlagd och avtalad
- [ ] Nätverkssegmentering: instrumentnät separerat från kontors-IT
- [ ] IoT-gateways (miljöövervakning) utan direkt molnanslutning — eller loggad
- [ ] BMS/SCADA-system identifierade och segmenterade

Kalibrering och dataintegritet

- [ ] Kalibreringsloggar skrivs till oföränderligt audit trail
- [ ] Hash-kedja eller motsvarande verifieringsmetod implementerad
- [ ] Inga instrument med utgånget kalibreringsintyg i drift
- [ ] Retroaktiv bedömning genomförd om kalibrerings-driftavvikelse inträffat

Incidenthantering och rapportering

- [ ] 72h-incidentprocess dokumenterad och testad
- [ ] OT-nätverkslogg aktiv med minst 12 månaders retention
- [ ] LIMS-events och BMS-larm korrelerade i gemensam logg
- [ ] Kontakt med CERT-SE / MSB etablerad och dokumenterad

CRA-förberedelse

- [ ] Inventering av instrument som klassas som Klass I, II eller IACS
- [ ] Leverantörers CRA-roadmap begärd för kritisk utrustning
- [ ] Plan för instrumentkonvertering inför aug 2027
- [ ] Patch-hanteringsprocess för OT-firmware dokumenterad

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