SITEWATCH SECURITY

GUIDE · REGELEFTERLEVNAD

NIS2 och CER: vad de nya kraven betyder för er fysiska säkerhet

Två regelverk skärper kraven på svenska samhällsviktiga verksamheter samtidigt. Här är vad de innebär för er fysiska säkerhet och åtkomst, vilka som omfattas, vilka datum som gäller, och en checklista att börja med.

För säkerhetsansvariga, fastighets- och driftchefer

Uppdaterad oktober 2026

DET HÄR FÅR DU UT AV GUIDEN

Två regelverk, samma mål

NIS2 och CER antogs av EU samtidigt i december 2022 och är avsiktligt två halvor av samma helhet. Det ena skyddar det digitala, det andra det fysiska. Vi reder också ut en vanlig förväxling: skillnaden mellan CER och CRA.

NIS2: cybersäkerhet

NIS2-direktivet genomförs i Sverige genom cybersäkerhetslagen, som trädde i kraft den 15 januari 2026. Lagen ställer hårdare krav på riskhantering, incidentrapportering och ledningens ansvar för ett brett spann av samhällsviktiga verksamheter. Verksamheter som omfattas ska anmäla sig så snart det kan ske. Sedan den 1 juli 2026 tar Nationellt cybersäkerhetscenter (NCSC) vid FRA emot anmälningarna, som tidigare gick till MCF. Utebliven anmälan kan leda till tillsynsåtgärder, och ändrade uppgifter ska anmälas inom 14 dagar.

> **Vad står på spel?** Tillsynsmyndigheterna kan besluta om sanktionsavgifter på upp till 10 miljoner euro eller 2 procent av global årsomsättning för väsentliga verksamhetsutövare, och upp till 7 miljoner euro eller 1,4 procent för viktiga. Lagen tydliggör dessutom ledningens personliga ansvar för säkerhetsarbetet.

CER: fysisk motståndskraft

CER-direktivet (kritiska entiteters motståndskraft) föreslås genomföras i Sverige genom en ny lag om motståndskraft hos kritiska verksamhetsutövare. Regeringen lämnade proposition 2025/26:303 till riksdagen den 14 juli 2026. Riksdagen har ännu inte beslutat, och lagen föreslås träda i kraft den 1 januari 2027. Där NIS2 handlar om cyber handlar CER om det fysiska och organisatoriska: skydd av anläggningar och lokaler, tillträdesskydd, personalsäkerhet, kontinuitet och förmågan att stå emot och återhämta sig från störningar, oavsett om de beror på intrång, sabotage, olyckor eller naturhändelser.

För er som arbetar med fysisk säkerhet är CER den viktiga nyheten. Där säkerhetsskyddslagen träffar ett smalt urval säkerhetskänsliga verksamheter får enligt förslaget ett brett spann av kritiska verksamheter uttryckliga krav på fysiskt skydd, till exempel tillträdesskydd, områdesövervakning och fysisk incidenthantering.

Och CRA då?

CRA (Cyber Resilience Act) blandas ofta ihop med CER, men är en helt annan sak. CRA är en EU-förordning som ställer cybersäkerhetskrav på produkter med digitala element, alltså själva kamerorna, sensorerna, gatewayerna och mjukvaran. Kraven riktar sig mot tillverkaren av produkten, inte mot er som verksamhet.

CRA trädde i kraft i december 2024. Rapporteringskraven för aktivt utnyttjade sårbarheter gäller sedan den 11 september 2026, och förordningen blir fullt tillämplig den 11 december 2027.

Vad det betyder för er: när ni upphandlar kameror, sensorer och larmsystem bör ni fråga leverantören hur produkterna lever upp till CRA. CER reglerar er motståndskraft, CRA reglerar utrustningen ni köper in. Tillsammans höjer de ribban för hela kedjan.

AVGRÄNSNING

Omfattas ni?

NIS2 omfattar väsentliga och viktiga entiteter inom sektorer som energi, transport, bankverksamhet, finansmarknad, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning, rymd, post, avfallshantering, kemikalier, livsmedel, tillverkning och vissa digitala tjänster. Som tumregel träffas medelstora och större organisationer, men det finns undantag åt båda håll.

Förslaget till CER-lag omfattar verksamhetsutövare som identifieras som kritiska. Tre kriterier föreslås gälla: ni tillhandahåller en eller flera samhällsviktiga tjänster, ni har kritisk infrastruktur i Sverige, och en störning skulle få betydande störande effekter på tjänsten.

Många verksamheter kan komma att omfattas av båda regelverken samtidigt. Är ni osäkra, utgå från att ni kan beröras och gör en avgränsningsanalys tidigt. Enligt förslaget görs den slutliga bedömningen för CER av svensk tillsynsmyndighet.

KÄRNAN

Vad kraven betyder för er fysiska säkerhet och åtkomst

Så här översätts regelverken till konkreta krav på den fysiska säkerheten.

Riskbedömning som omfattar fysiska hot

Ni ska regelbundet bedöma alla relevanta hot, inte bara digitala. Det inkluderar intrång, sabotage, manipulation av utrustning, insiderhot och numera även drönare över känsliga ytor.

Skydd av anläggningar och perimeter

Lokaler, områden och kritisk utrustning ska skyddas. I praktiken handlar det om perimeterskydd, områdesövervakning, tillträdesbegränsning och förmåga att upptäcka obehörig närvaro innan skada sker.

Åtkomstkontroll och behörigheter

Vem får vara var, när och hur det loggas. Tillträde till känsliga utrymmen ska styras, dokumenteras och kunna granskas i efterhand.

Detektion i realtid

NIS2 kräver en tidig varning inom 24 timmar. Den fristen går inte att hålla med system som bara spelar in för granskning i efterhand. I praktiken måste ni veta att något hänt i samma stund som det händer.

Incidenthantering och rapportering

Ni ska kunna upptäcka, klassificera, hantera och rapportera incidenter inom satta tidsfrister. NIS2 kräver en tidig varning inom 24 timmar och en incidentanmälan inom 72 timmar. Sedan den 1 juli 2026 rapporteras incidenter till NCSC, som vidarebefordrar dem till berörd tillsynsmyndighet.

Spårbarhet och loggning

Händelser, larm och åtkomst ska loggas och bevaras så att de kan användas som underlag vid utredning, revision och rapportering. Spårbarhet är genomgående i båda regelverken.

Personalsäkerhet och leverantörskedja

Bakgrund, behörigheter och rutiner för personal med tillträde till känsliga miljöer, samt koll på de leverantörer och system ni är beroende av.

Kontinuitet och återhämtning

Förmåga att upprätthålla eller snabbt återställa verksamheten efter en störning, med redundans där det behövs.

DATUM ATT HÅLLA KOLL PÅ

Tidslinje och deadlines

15 januari 2026	Cybersäkerhetslagen (NIS2) trädde i kraft.
2 februari 2026	Anmälan enligt lagen öppnade. Den ska göras så snart det kan ske.
11 juni 2026	CRA:s regler om anmälda organ började gälla.
1 juli 2026	Föreskrifterna om incidentrapportering (MCFFS 2026:8) trädde i kraft. Samma dag flyttade cyberverksamheten från MCF till NCSC vid FRA, som nu tar emot anmälningar och incidentrapporter.
11 september 2026	CRA:s rapporteringskrav för sårbarheter och allvarliga incidenter började gälla.
1 oktober 2026	Föreskrifterna om säkerhetsåtgärder och ledningens utbildning (MCFFS 2026:11) trädde i kraft.
1 januari 2027	Den svenska CER-lagen föreslås träda i kraft. Riksdagen har ännu inte beslutat.
11 december 2027	CRA blir fullt tillämplig för produkter på EU-marknaden.

KOM IGÅNG

Checklista: fysiska säkerhetsåtgärder att börja med

- ✓ Kartlägg om ni omfattas av NIS2, CER eller båda, och av vilken tillsynsmyndighet.
- ✓ Anmäl er till NCSC vid FRA om ni inte redan har gjort det. Anmälan ska göras så snart det kan ske och har ingen framtida deadline att vänta på.
- ✓ Gör en riskbedömning som uttryckligen omfattar fysiska hot mot anläggningar och utrustning.
- ✓ Inventera perimeter och tillträdesskydd: var kan någon ta sig in oupptäckt?
- ✓ Säkerställ åtkomstkontroll till känsliga utrymmen, med behörigheter och logg.
- ✓ Inför detektion i realtid, så att händelser larmar i stunden och inte bara spelas in.
- ✓ Etablera en incidentprocess som klarar 24- och 72-timmarsfristerna i NIS2.
- ✓ Säkra spårbarhet: loggar och händelsedata ska bevaras och gå att ta fram.
- ✓ Samla säkerhet och drift i en gemensam lägesbild så att inget faller mellan systemen.
- ✓ Ställ CRA-frågan till era leverantörer av kameror, sensorer och larm.
- ✓ Kontrollera var er säkerhetsdata lagras och vem som har tillgång till den.
- ✓ Dokumentera allt. Det ni inte kan visa upp räknas inte vid en tillsyn.

UNDVIK FALLGROPARNA

Vanliga misstag

Att se NIS2 som ett rent it-projekt och glömma den fysiska sidan. Förslaget till CER-lag adresserar den luckan, och fysisk och digital säkerhet behöver hanteras ihop.

Att förlita sig på inspelning i efterhand. Bevis efter en händelse uppfyller inte kravet på att upptäcka och agera i realtid.

Att ha säkerhet och drift i skilda system. Det gör incidenthantering och rapportering långsam, precis när tidsfristerna kräver snabbhet.

Att vänta. Anmälningsplikten gäller redan nu, och åtgärder på fysisk säkerhet tar tid att upphandla och installera.

Så stödjer en eventbaserad plattform kraven

Sitewatch samlar kameror, sensorer, larm och passersystem i en gemensam vy och agerar på händelser i realtid. Det stödjer flera av kraven ovan: detektion i stunden, samlad åtkomst- och händelselogg för spårbarhet, snabbare underlag för incidentrapportering och en samlad lägesbild för säkerhet och drift. Ingen säkerhetsdata lämnar EU. Drift och lagring sker hos svensk hostingleverantör.

Plattformen gör er inte automatiskt regelefterlevande, ansvaret ligger hos er, men den ger er verktygen som flera av kraven förutsätter. Vill ni veta hur det ser ut i er miljö, boka en genomgång så kopplar vi er till rätt partner.

KÄLLOR OCH FÖRDJUPNING

- Nationellt cybersäkerhetscenter (NCSC) vid FRA om cybersäkerhetslagen (NIS2), anmälan och föreskrifter.
- Regeringen, prop. 2025/26:303 ”En ny lag för ökad motståndskraft hos kritiska verksamhetsutövare” (2026).
- EU-kommissionen om Cyber Resilience Act (CRA).

Den här guiden är en översikt, inte juridisk rådgivning. Stäm av er specifika situation med er tillsynsmyndighet eller juridiska rådgivare. Riksdagen har ännu inte beslutat om den svenska CER-lagen. © 2026 Sitewatch AB.

Sitewatch AB · sitewatch.se/boka-demo · info@sitewatch.se · 010-540 81 30