NISCHOMRÅDE · KURERAD TRENDANALYS

NIS2 och CER-resiliens för kritisk infrastruktur

Nischområdet omfattar rådgivning och lösningar för verksamhetsutövare av kritisk infrastruktur att uppfylla kraven i NIS2- och CER-direktiven gällande cybersäkerhet, fysisk resiliens och regelefterlevnad, för att undvika sanktionsavgifter.

UPPDATERAD 29 juni 2026

Mikro Makro Mega

12
PUBLICERADE TRENDER

© Trendscope · version 5 · 2026-08-08 · 1/14

MAKROTREND

Integrerad fysisk och digital resiliens för kritisk infrastruktur

CER-direktivet (fysisk resiliens) och NIS2-direktivet (cybersäkerhet) är nära sammankopplade och driver en gemensam strategi för att stärka samhällets motståndskraft. Detta innebär att organisationer, särskilt inom energisektorn, måste hantera både fysiska hot (extremväder, sabotage) och digitala hot (cyberattacker) på ett integrerat sätt, med skärpta krav på governance, riskhantering och incidenthantering för att skydda både fysiska tillgångar och digitala system.

Sakerhet | Digitalisering | Infrastruktur | 4 observationer · senast 1 augusti 2026

Källor

01 **[PDF] Tillsammans elektrifierar vi Sverige - Ellevio**
ellevio.se

02 **CER-direktivet | Vad är det och vad innebär det för dig? | RISMA**
rismasystems.com

03 **NIS2: Förstå vad som är viktigt nu - inspelat webinar | Conscia Sverige**
conscia.com

MAKROTREND

Implementering av CER-direktivet för skydd av kritisk infrastruktur

Myndigheten för civilt försvar (MSB) förbereder genomförandet av EU:s CER-direktiv (Resilience of Critical Entities Directive). Detta direktiv kräver att företag inom kritiska sektorer utför riskbedömningar för att hantera hot som naturhändelser, olyckor, folkhälsa, antagonistiska hot och hybridhot, vilket skapar ett behov av nya säkerhetslösningar och konsulttjänster.

Reglering | Sakerhet | Infrastruktur | 4 observationer · senast 28 maj 2026

Källor

01 **Myndigheten för civilt försvar ska förbereda genomförandet av CER ...**
mcf.se

02 **Översvämningar och kritisk infrastruktur - Sweco Sverige**
sweco.se

03 **CER-direktivet | Vad är det och vad innebär det för dig? | RISMA**
rismasystems.com

© Trendscope · version 5 · 2026-08-08 · 3/14

MAKROTREND

Förstärkt ledningsansvar och 'whole-entity approach' med NIS2

Den nya svenska cybersäkerhetslagen, som implementerar NIS2-direktivet från januari 2026, utökar cybersäkerhetsansvaret till 18 kritiska sektorer och kräver ett 'whole-entity approach'. Detta innebär att ansvaret sträcker sig över hela organisationen, inte bara specifika IT-system, och ledningen kan hållas personligen ansvarig för intrång. Företag måste nu fokusera på systematiskt cybersäkerhetsarbete, riskbedömning, implementering av säkerhetsåtgärder och obligatorisk incidentrapportering.

Reglering | Sakerhet | Arbetskraft | 4 observationer · senast 28 maj 2026

Källor

01 **[PDF] förändringar i EU:s cybersäkerhetsakt och i NIS 2-direktivet**
regeringen.se

02 **Blogg NIS2 Sverige 2026**
balrconsulting.com

03 **A New Cybersecurity Act Swedens Implementation of NIS2**
deloitte.com

© Trendscope · version 5 · 2026-08-08 · 4/14

MAKROTREND

Behov av cybersäkerhetskompetens hos privata aktörer

Den nya cybersäkerhetslagen (NIS2), som införs i januari 2026, ställer omfattande krav på systematiskt cybersäkerhetsarbete, riskanalyser och incidentrapportering för privata aktörer inom 18 samhällsviktiga sektorer. Detta kommer att skapa en betydande efterfrågan på specialistkompetens inom cybersäkerhet och riskhantering för att säkerställa regelefterlevnad och skydda digitala tillgångar.

Reglering | Sakerhet | Arbetskraft | 10 observationer · senast 2 juni 2026

Källor

01 **NIS 2-direktivet: säkra nätverks- och informationssystem**
digital-strategy.ec.europa.eu

02 **New Cybersecurity Act Enters Into Force in Sweden**
energimyndigheten.se

03 **Det här gäller för nya cybersäkerhetslagen - Finansinspektionen**
fi.se

© Trendscope · version 5 · 2026-08-08 · 5/14

MAKROTREND

Förstärkt reglering av kritisk infrastruktur (CER-direktivet)

EU:s CER-direktiv (Critical Entities Resilience Directive) ersätter äldre reglering och utökar omfattningen till elva sektorer, inklusive energi, transport och digital infrastruktur. Detta innebär att svenska företag inom dessa sektorer kommer att behöva genomföra omfattande riskbedömningar och implementera åtgärder för att stärka sin förmåga att motstå, hantera och återhämta sig från allvarliga incidenter, oavsett orsak. Direktivet förväntas träda i kraft i svensk lag under 2026.

Reglering | Sakerhet | Infrastruktur | 9 observationer · senast 28 maj 2026

Källor

01 **Sverige ska bygga motståndskraft i samhällsviktig verksamhet**
regeringen.se

02 **Digital operativ motståndskraft för finanssektorn - Riksdagen**
riksdagen.se

03 **Nya Cybersakerhetslagen Borjar Galla Sa Paverkas Foretagen**
svensktnaringsliv.se

© Trendscope · version 5 · 2026-08-08 · 6/14

MEGATREND

Skärpta krav på cybersäkerhet genom NIS 2

Implementeringen av NIS 2-direktivet och nya nationella säkerhetskrav ökar kraven på informationssäkerhet för företag som hanterar samhällsviktig datainfrastruktur. Detta driver investeringar i säkra molnlösningar och robusta nätverk.

Sakerhet | Reglering | 20 observationer · senast 28 maj 2026

Källor

01 **Uppdrag till Myndigheten för samhällsskydd och beredskap att ...**
regeringen.se

02 **NIS2: EU:s nya direktiv för cybersäkerhet | CGI Sverige**
cgi.com

03 **Nyheter & Event | Datacom**
datacom.se

© Trendscope · version 5 · 2026-08-08 · 7/14

MAKROTREND

NIS2 / svensk cybersäkerhetslag kräver incidentrapportering och riskstyrning för bokningsplattformar

NIS2-transpositionen i Sverige inför skyldigheter för ’väsentliga’ och ’viktiga’ digitala tjänster — inklusive vissa bokningssystem och plattformsdrift — att införa riskhantering, incidentrapporteringsrutiner och ledningsansvar. Praktiskt: klassificera era system, bygg 72-timmars incidentprocesser och dokumentera säkerhetsåtgärder (svensk lag trädde i kraft 15 jan 2026 i transponerad form).

Sakerhet | Reglering | Digitalisering | 10 observationer · senast 28 maj 2026

Källor

01 **Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag (Proposition 2025/26:28) | Sveriges riksdag**
riksdagen.se

02 **New Cybersecurity Act Enters Into Force in Sweden**
energimyndigheten.se

03 **Cybersäkerhetslagen 2026: NIS2-direktivet i Sverige - Tech Insider**
tech-insider.org

© Trendscope · version 5 · 2026-08-08 · 8/14

MAKROTREND

Utökad tillämpning av cybersäkerhetskrav enligt NIS2

Den nya cybersäkerhetslagen, som implementerar EU:s NIS2-direktiv, utökar omfattningen av reglerade sektorer till 18 och tillämpar krav på hela organisationer. Detta innebär att fler företag, även utanför traditionellt kritiska sektorer, måste implementera riskbaserade säkerhetsåtgärder och rapportera incidenter, vilket skapar ett ökat behov av cybersäkerhetstjänster och -lösningar.

Reglering | Sakerhet | Konkurrens | 9 observationer · senast 28 maj 2026

Källor

01 **New Cybersecurity Act Enters Into Force in Sweden**
energimyndigheten.se

02 **NIS2, cybersäkerhetslagen och DORA i finanssektorn - TechLaw**
techlaw.se

03 **DORA vs NIS2: Skillnader, Krav och Lösningar - Cosafe**
cosafe.com

© Trendscope · version 5 · 2026-08-08 · 9/14

MAKROTREND

Sektorsövergripande resiliens mot naturkatastrofer och sabotage

CER-direktivet breddar fokus från enbart antagonistiska hot till att även inkludera naturkatastrofer, pandemier och olyckor. Detta tvingar företag att utveckla mer robusta kontinuitetsplaner som kan hantera fysiska avbrott i kritisk infrastruktur, vilket skapar en ny marknad för konsulttjänster inom fysisk resiliens och krishantering.

Sakerhet | Hallbarhet | Infrastruktur | 2 observationer · senast 28 maj 2026

Källor

01 **Ökad motståndskraft hos kritiska verksamhetsutövare (CER)**
transportstyrelsen.se

02 **CER-direktivet - Energimyndigheten**
energimyndigheten.se

03 **Om CER-direktivet - Energiföretagen Sverige**
energiforetagen.se

© Trendscope · version 5 · 2026-08-08 · 10/14

MAKROTREND

NIS2 / svensk cybersäkerhetslag gör hotell och bokningskedjor ansvariga – fokus på leverantörskedjan

NIS2-implementering i Sverige (ny cybersäkerhetslag) innebär registrering, incidentrapportering och förstärkta krav för verksamheter som klassas som väsentliga eller viktiga; bokningsmotorer, betalväxlar och större hotell kan omfattas. Konkreta åtgärder är att kartlägga scope, införa incident- och eskaleringsrutiner, uppgradera loggning/backups och ställa krav i leverantörsavtal för att minska tredjeparts-exponering.

Sakerhet | Digitalisering | Logistik | 13 observationer · senast 28 maj 2026

Källor

01 **Timeline for the Implementation of the EU AI Act | AI Act Service Desk**
ai-act-service-desk.ec.europa.eu

02 **NIS2 och ny cybersäkerhetslag - Energiföretagen Sverige**
energiforetagen.se

03 **Bostadsrätterna | Ny lag om andrahandsuthyrning klar**
bostadsratterna.se

© Trendscope · version 5 · 2026-08-08 · 11/14

MAKROTREND

NIS2 och svensk cybersäkerhetsimplementering: formalisera cyber-governance och incidenthantering

NIS2 breddar ansvar för cyberresiliens och kräver formella riskanalyser, ledningsansvar, leverantörskrav och snabb incidentrapportering — PMS, bokningsmotorer, betalväxlar och centrala IT-leverantörer kan omfattas. Hotell måste bygga styrmodell för leverantörsstyrning, implementera loggning/övervakning och öva incident-rutiner samt uppdatera styrelsens ansvar och rapporteringskedjor inför nationell implementering 2025–2026.

Sakerhet | Digitalisering | 14 observationer · senast 28 maj 2026

Källor

01 **AI Act | Shaping Europe's digital future**
digital-strategy.ec.europa.eu

02 **NIS2 i Sverige 2026: Komplett guide för svenska bolag**
balrconsulting.com

03 **Stärkta krav på cybersäkerhet: Detta är NIS2 | AJG Sverige**
ajg.com

© Trendscope · version 5 · 2026-08-08 · 12/14

MAKROTREND

Harmonisering av nationell tillsyn och sanktionssystem

Sverige genomför nu en omfattande anpassning av svensk rätt för att synkronisera NIS2 och CER med säkerhetsskyddslagen. Detta skapar en mer förutsägbar men striktare tillsynsmiljö där myndigheter (t.ex. MSB, Energimyndigheten) får utökade befogenheter att utföra inspektioner och säkerhetsrevisioner.

Politik | Sakerhet | Reglering | 1 observation · senast 28 maj 2026

Källor

01 **[PDF] Genomförande av EU:s direktiv om åtgärder för en hög gemensam ...**
regeringen.se

02 **Det här är cybersäkerhetslagen**
mcf.se

03 **NIS-direktivet - SKR**
skr.se

OM ANALYSEN

Använd gärna analysen

Du får gärna skriva ut, dela och citera ur analysen. Använd insikterna i ert eget arbete, i presentationer och i samtal där de kan göra nytta.

DOKUMENTKÄLLA

https://trendscope.se/nis2-och-cer-resiliens-for-kritisk-infrastruktur

NÄR DU HÄNVISAR

Ange Trendscope som källa. I digitala sammanhang får du gärna länka tillbaka till dokumentkällan, så att läsaren kan hitta den senaste publicerade versionen och följa underlaget vidare.

KONTROLLERA VIKTIGA UPPGIFTER

Både människor och AI kan missa sammanhang, feltolka uppgifter eller återge en källa fel. Kontrollera därför originalkällan när en uppgift ska ligga till grund för beslut, publicering eller andra sammanhang där korrekthet är viktig.

AI-STÖD OCH MÄNSKLIG KURERING

Delar av källinsamlingen och bearbetningen har gjorts med AI-stöd. Urval, struktur och den publicerade analysen har granskats och kurerats redaktionellt av människor.

FÖRESLAGEN HÄNVISNING

Trendscope. “NIS2 och CER-resiliens för kritisk infrastruktur”. Uppdaterad 29 juni 2026.

© Trendscope · version 5 · 2026-08-08 · 14/14