NISCHOMRÅDE · KURERAD TRENDANALYS

Efterlevnad av NIS2-direktivet för små och medelstora företag

Fokus på hur små och medelstora företag i kritiska sektorer uppfyller NIS2-direktivets krav på cybersäkerhet, riskhantering och incidentrapportering i Sverige.

UPPDATERAD 13 augusti 2026

Mikro Makro Mega

12
PUBLICERADE TRENDER

© Trendscope · version 5 · 2026-08-13 · 1/15

KORT SVAR

Det viktigaste i analysen

NIS2-direktivet innebär att ledningen i små och medelstora företag nu bär ett personligt ansvar för cybersäkerhet genom ett **förstärkt ledningsansvar**. För att möta kraven krävs ett systematiskt arbete som omfattar hela organisationen, inklusive **säkerhet i leverantörskedjan** och dokumenterad riskhantering.

01 Vilket ansvar vilar på ledningen enligt NIS2?

Ledningen har ett direkt personligt ansvar för cybersäkerhetsarbetet genom ett **whole-entity approach**. Detta innebär att de måste säkerställa att riskbedömningar och säkerhetsåtgärder är integrerade i hela verksamheten.

02 Hur bör vi prioritera våra investeringar i säkerhet?

Prioritera investeringar i **standardiserade ramverk**. Dessa ger en strukturerad mall för efterlevnad som är avgörande för att säkra framtida **finansiering**.

03 Vilka risker finns i vår leverantörskedja?

Tredjepartsrisker är en kritisk punkt under NIS2. Ni måste ställa krav i leverantörsavtal och implementera **Zero Trust-arkitektur** för att minska exponeringen i leverantörskedjan.

04 Hur hanterar vi bristen på intern cybersäkerhetskompetens?

Outsourca säkerhetsoperationer till en **Managed Security Service Provider**. Detta ger tillgång till den expertis som krävs för att möta det ökade **behovet av cybersäkerhetskompetens**.

© Trendscope · version 5 · 2026-08-13 · 2/15

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 · 2026-08-13 · 3/15

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 · 2026-08-13 · 4/15

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 | 14 observationer · senast 9 augusti 2026

Källor

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

02 **Vad innebär NIS2? | Nexer**
nexergroup.com

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

© Trendscope · version 5 · 2026-08-13 · 5/15

MIKROTREND

Standardiserade ramverk som efterlevnadsstöd

Eftersom NIS2 inte föreskriver en specifik teknisk lösning, ökar adoptionen av etablerade ramverk som ISO 27001, NIST CSF och CIS Controls bland SME. Dessa fungerar som en 'best practice'-mall för att strukturera riskhantering och dokumentation inför tillsyn.

Sakerhet | Kvalitet | Effektivisering | 1 observation · senast 28 maj 2026

Källor

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

02 **NIS2 Directive Why Small Businesses Cant Afford To Ignore It Anymore**
webristle.com

03 **Germanys New NIS2 Cybersecurity Law**
secfix.com

© Trendscope · version 5 · 2026-08-13 · 6/15

MAKROTREND

Stärkt regelefterlevnad och dataskydd för SMB drivet av NIS2 och GDPR

Nya och uppdaterade lagar som GDPR och det kommande NIS2-direktivet ställer ökade krav på dataskydd och informationssäkerhet för SMB. Detta tvingar företag att inte bara efterleva befintliga regler utan också förbereda sig för nya, vilket inkluderar att säkra verksamheten utan att behöva anställa fast personal, samt att hantera rättsliga konsekvenser och förlorat förtroende vid bristande efterlevnad.

Reglering | Sakerhet | Digitalisering | 2 observationer · senast 28 maj 2026

Källor

01 **Informations- och cybersäkerhet - Sweco Sverige**
sweco.se

02 **Program | GTC Konferensen 2025**
gtcc.se

03 **NIS2-direktivet i Sverige — krav, sektorer och deadlines**
webbfabriken.com

© Trendscope · version 5 · 2026-08-13 · 7/15

MIKROTREND

Fokus på säkerhet i digitala leveranskedjor för små och medelstora företag

MSB (Myndigheten för samhällsskydd och beredskap) finansierar projekt för att stärka säkerheten i digitala leveranskedjor, särskilt riktade mot små och medelstora företag (SME). Detta syftar till att bygga ett mer motståndskraftigt samhälle genom att adressera sårbarheter i hela ekosystemet, vilket indikerar ett ökat fokus på helhetssäkerhet bortom de stora aktörerna.

Logistik | Sakerhet | Effektivisering | 4 observationer · senast 28 maj 2026

Källor

01 **[PDF] Bilaga 1 Handlingsplan Uppdaterad 2026**
regeringen.se

02 **msb.se**
ncc-se.msb.se

03 **Syna Regeringens Cybermiljard**
techsverige.se

© Trendscope · version 5 · 2026-08-13 · 8/15

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 · 2026-08-13 · 9/15

MIKROTREND

Cybersäkerhetsmognad som villkor för finansiering

För SME och startups inom kritiska sektorer blir dokumenterad efterlevnad av NIS2-ramverk en avgörande faktor för att säkra venture capital och bankfinansiering. Investerare ser nu säkerhetsbrister som en direkt finansiell risk som kan påverka bolagets värdering och överlevnad.

Ekonomi | Sakerhet | Innovation | 1 observation · senast 28 maj 2026

Källor

01 **Top Compliance Frameworks Every EU Fintech Startup Must Know in 2026**
defendsphere.io

02 **NIS2 Compliance For Smes**
spanishcomplianceinstitute.com

© Trendscope · version 5 · 2026-08-13 · 10/15

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 · 2026-08-13 · 11/15

MAKROTREND

Zero Trust-arkitektur som standard för små leverantörer

Kravet på leveranskedjesäkerhet driver en snabb adoption av Zero Trust-principer även hos mindre företag. För att behålla sin roll som underleverantörer till kritiska sektorer tvingas SME implementera striktare åtkomstkontroll och loggning, vilket i praktiken höjer den generella säkerhetsnivån i hela det svenska näringslivets digitala infrastruktur.

Teknik | Digitalisering | Sakerhet | 1 observation · senast 28 maj 2026

Källor

01 **NIS2 i Sverige – hur påverkas din verksamhet? - GlobalConnect**
foretag.globalconnect.se

02 **[PDF] Från NIS1 till NIS2 - Lund University Publications**
lup.lub.lu.se

© Trendscope · version 5 · 2026-08-13 · 12/15

MIKROTREND

RegTech och SupTech för DORA/NIS2-efterlevnad

Den komplexa och överlappande regleringen från DORA och NIS2 driver fram innovation inom RegTech (Regulatory Technology) och SupTech (Supervisory Technology). Företag kommer att investera i lösningar för att automatisera efterlevnad, incidentrapportering och riskhantering, samt för att underlätta tillsyn.

Reglering | Digitalisering | Effektivisering | 2 observationer · senast 28 maj 2026

Källor

01 **Viktiga Nyheter Informationssakerhet**
stratsys.com

02 **[PDF] Report Fortinet Banking Regulations**
fortinet.com

03 **Omfattas ni av NIS2? Krav och sektorer - ChainSec**
chainsec.se

© Trendscope · version 5 · 2026-08-13 · 13/15

MIKROTREND

Ökad efterfrågan på outsourcad incidentrespons och säkerhetsoperationer

Många små och medelstora företag (SME) och medelstora företag saknar intern kapacitet för att hantera den ökande komplexiteten i cybersäkerhet. Detta driver en trend där de i allt högre grad outsourcar sina säkerhetsoperationer, inklusive hotövervakning och incidentrespons, till Managed Security Service Providers (MSSP). Denna trend förstärks av NIS2-krav på obligatorisk incidentrapportering, vilket kräver robusta rutiner för incidenthantering.

Affarsmodeller | Sakerhet | Effektivisering | 4 observationer · senast 28 maj 2026

Källor

01 **[PDF] The Swedish Market For Cybersecurity**
kommerskollegium.se

02 **NIS2-direktivet och cybersäkerhetslagen 2026 - Lawbox**
lawbox.se

03 **vad innebär nis2 och cybersäkerhetslagen? - Nexer**
nexergroup.com

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/efterlevnad-av-nis2-direktivet-for-sma-och-medelst-2

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. “Efterlevnad av NIS2-direktivet för små och medelstora företag”. Uppdaterad 13 augusti 2026.

© Trendscope · version 5 · 2026-08-13 · 15/15