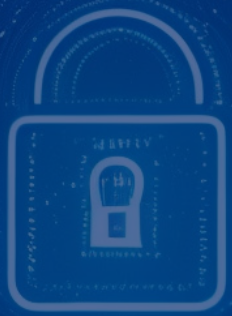
Så förbereder ni er verksamhet
för det nya EU-direktivet

Introduktion till det nya NIS 2-direktivet

Av CANEA



CANEA

EU-direktivet NIS 2 som börjar gälla under 2025 är en utvidgning av det ursprungliga NIS – Network and Information Systems Directive – från 2016. Organisationer som omfattas av direktivet, samt leverantörer till dessa, bör förbereda sig för de nya kraven i tid. ISO 27001 och dess systerstandarder kan med fördel användas som grund för ett systematiskt arbete med informationssäkerhet i syfte att uppfylla de utvidgade kraven i NIS 2.

Bakgrund

NIS-direktivet som trädde i kraft den 19 juli 2016 är en EU-reglering som syftar till att höja den allmänna nivån av cybersäkerhet och säkerställa en hög säkerhetsnivå för samhällskritisk infrastruktur och viktiga tjänster. NIS 2-direktivet är en uppdatering av det ursprungliga NIS-direktivet och börja gälla som lag i Sverige under 2025. NIS 2-direktivet omfattar fler sektorer och organisationer, innebär strängare säkerhetskrav och rapporteringsförpliktelser samt stärker tillsynsmyndigheternas befogenheter och samarbetet mellan medlemsstaterna.

För att förbereda sig inför NIS 2 bör organisationer som omfattas av direktivet genomföra en riskanalys och -bedömning av sin informations- och cybersäker-

hetsstatus för att identifiera eventuella brister mot kraven i NIS 2. Några av de konkreta åtgärder som kan behöva införas innefattar bland annat stärkt säkerhetsmedvetenhet inom organisationen, kontinuitetsplanering, förstärkta informationssäkerhetsåtgärder, utökat samarbete med andra aktörer samt ett mer systematiskt arbete med uppföljning och förbättring av informationssäkerheten.

Den internationella standarden ISO 27001:2022 är en utmärkt grund för ett ledningssystem för informations- och cybersäkerhet som inte bara uppfyller de specifika kraven i NIS 2-direktivet utan även förbättrar det övergripande förhållningssättet och motståndskraften mot cybersäkerhetshot.

Om det ursprungliga NIS-direktivet

NIS-direktivet (EU 2016/1148), även kallat direktivet om säkerhet för nätverks- och informationssystem är EU:s första omfattande lagstiftning avsedd att stärka cybersäkerheten inom unionen. Direktivet syftar till att höja medlemsstaternas allmänna nivå av cybersäkerhet, skydda kritisk infrastruktur och säkerställa en hög gemensam säkerhetsnivå för nätverk och informationssystem inom EU. Direktivet antogs av Europaparlamentet och Europeiska rådet och trädde i kraft den 19 juli 2016.

NIS-direktivet riktar sig huvudsakligen till två grupper av organisationer. Den första gruppen utgörs av leverantörer av samhällskritiska tjänster (OES) inom områden som energi, transport, bankväsen, hälso- och sjukvård, dricksvattenförsörjning och digital infrastruktur. Den andra gruppen utgörs av leverantörer av vissa typer av digitala tjänster (DSP), såsom molntjänster, sökmotorer och online-marknadsplatser.

Organisationer som levererar tjänster inom dessa områden är enligt NIS-direktivet skyldiga att vidta lämpliga tekniska och organisatoriska skyddsåtgärder för att hantera cybersäkerhetsrisker samt rapportera allvarliga incidenter till nationella myndigheter.

Om det nya NIS 2-direktivet

NIS 2-direktivet är en uppdatering av det ursprungliga NIS-direktivet. Uppdateringen trädde i kraft i januari 2023 på EU-nivå och börja gälla som lag i Sverige under 2025. NIS 2-direktivet togs fram för att hantera det ständigt föränderliga cybersäkerhetslandskapet samt för att ta itu med de brister som identifierats i genomförandet av det ursprungliga direktivet. NIS 2 omfattar bland annat fler sektorer och organisationer, inför strängare säkerhetskrav och rapporteringsförpliktelser, samt stärker tillsynsmyndigheternas befogenheter och samarbetet mellan medlemsstaterna. Det vidgade tillämpningsområdet och de förstärkta kraven gör att NIS 2-direktivet bidrar till en förbättrad och mer enhetlig cybersäkerhetsstandard inom hela EU. Den svenska regeringen har tillsatt en utredning av genomförandet av NIS 2-direktivet samt EU:s direktiv om kritiska entiteters motståndskraft (CER), vilket är en del av arbetet med att införliva direktivet i svensk lagstiftning.

BERÖRDA ORGANISATIONER

NIS 2-direktivet omfattar en bredare krets av organisationer och sektorer. Organisationerna som omfattas av NIS 2 delas fortfarande in i två huvudsakliga grupper: “Operatörer av väsentliga tjänster (OES)”, samt “Viktiga enheter”. Gruppen “viktiga enheter” gick tidigare under benämningen ”Leverantörer av digitala tjänster (DSP)”.
Tabellerna nedan visar de typer av organisationer som ingår i dessa grupper samt exempel på organisationer av varje typ.

Operatörer av väsentliga tjänster	Exempel
Energi	Elproducenter samt -distributörer och -transmissionsoperatörer; gasproducenter samt -transportörer och -distributörer; oljedistributörer.
Transport	Flygplatser, hamnar, järnvägsinfrastruktur, trafikstyrning.
Bank	Kreditinstitut såsom banker.
Finans	Börser, klareringshus.
Hälso- och sjukvård	Sjukhus, laboratorier, akutsjukvård.
Dricksvattenförsörjning	Vattenverk och distributionsnät.
Digital infrastruktur	Internetväxlar, domännamnsystem (DNS)-tjänster.
Offentlig administration	Myndigheter och förvaltningar på nationell, regional och kommunal nivå.
Livsmedelssektor	Livsmedelsproduktion och -distribution.
Tillverkning av kritiska produkter	Tillverkning av läkemedel, medicinsk utrustning, elektronik, kemikalier.

Viktiga enheter	Exempel
Digitala tjänster	Molntjänstleverantörer, sökmotorer, online-marknadsplatser.
Post- och kurirtjänster	Postdistribution, paketleverans.
Avfallshantering	Hantering av farligt avfall, återvinning.
Kemikalier	Kemisk produktion och distribution.
Livsmedel	Livsmedelsproduktion och -distribution med hög relevans för offentlig försörjning.
Rymd	Satellitoperatörer, rymdinfrastruktur.
Forskning	Forskningsinstitut med fokus på kritisk infrastruktur och tjänster.
Offentlig administration	Myndigheter och förvaltningar på nationell, regional och kommunal nivå.
Livsmedelssektor	Livsmedelsproduktion och -distribution.
Tillverkning av kritiska produkter	Tillverkning av läkemedel, medicinsk utrustning, elektronik, kemikalier.

VAD GÄLLER FÖR LEVERANTÖRER?

Leverantörer till organisationer som omfattas av NIS 2-direktivet spelar en kritisk roll i cybersäkerhetskedjan. Även om leverantörerna i sig inte alltid direkt omfattas av NIS 2-direktivet på samma sätt som de primärt reglerade organisationerna, ställer direktivet krav på att dessa organisationer hanterar cybersäkerhetsrisker i sina leveranskedjor. Det innebär att organisationer som omfattas av NIS 2 behöver säkerställa att även leverantörer upprätthåller en hög säkerhetsstandard för att skydda sig mot cybersäkerhetshot. När det gäller leverantörer till organisationer som omfattas av NIS 2 bör bland annat följande delar beaktas:

Riskhantering
Organisationer som omfattas av NIS 2 måste bedöma och hantera risker kopplade till sin informations- och kommunikationsteknik samt sina leveranskedjor. Detta innebär att det finns ett indirekt krav på att leverantörer måste uppfylla säkerhetsstandarder som följs av de reglerade organisationerna.

Kontraktsmässiga skyldigheter
För att uppfylla direktivets krav, kan organisationerna behöva inkludera specifika säkerhetskrav i sina kontrakt med leverantörer. Dessa krav kan omfatta åtgärder för cybersäkerhet, incidentrapportering och regelbunden säkerhetsgranskning.

Övervakning och granskning
Organisationer som omfattas av direktivet förväntas övervaka och, vid behov, granska sina leverantörers efterlevnad av de uppsatta säkerhetskraven. Detta kan innebära att man utför säkerhetsbedömningar eller revisioner av leverantörernas system och processer.

Incidentrapportering
I händelse av en cybersäkerhetsincident som påverkar en leverantör och som i sin tur kan påverka den reglerade organisationen, förväntas organisationen inkludera detta i sin incidentrapportering till de relevanta nationella tillsynsmyndigheterna. Därmed är det viktigt att ha tydliga protokoll och kommunikationsvägar med leverantörer gällande hantering och rapportering av säkerhetsincidenter.

Även om leverantörer till organisationer som omfattas av NIS 2-direktivet inte direkt regleras av direktivet, krävs det alltså indirekt att de uppfyller de säkerhetskrav och standarder som deras kunder, de reglerade organisationerna, måste uppfylla. Det är upp till de organisationer som omfattas av direktivet att säkerställa att deras leverantörer har adekvata cybersäkerhetsåtgärder på plats.

FÖRÄNDRINGAR MELLAN NIS OCH NIS 2

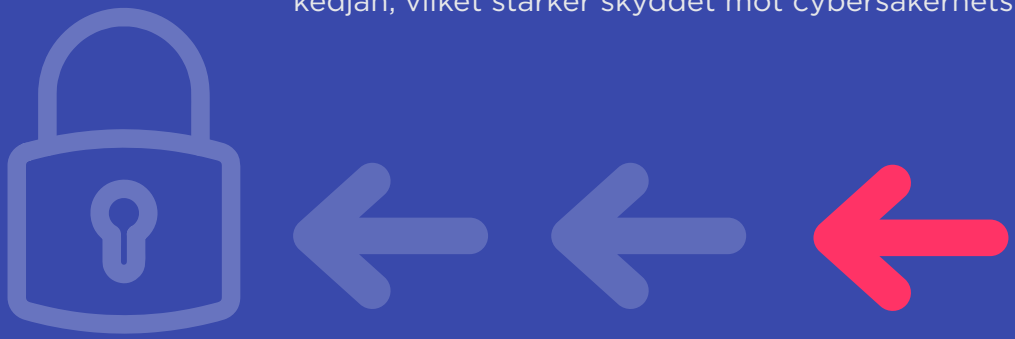
En jämförelse mellan det ursprungliga NIS-direktivet och det nya NIS 2-direktivet visar på både en uppstramning av kraven och en utvidgning av de organisationer som omfattas av direktivet. Några av de viktigaste förändringarna mellan NIS och NIS 2 innefattar bland annat följande (se även bilaga 1 för mer detaljer):

Tillämpningsområde
Den mest framträdande förändringen är utvidgningen av tillämpningsområdet; NIS fokuserade på specifika sektorer och digitala tjänster, medan NIS 2 inkluderar ett bredare spektrum av sektorer som offentlig förvaltning och livsmedelssektor, för att inkludera det ökande beroendet av digital infrastruktur.

Risk och incidenthantering
NIS 2 ställer högre krav på riskhantering och incidentrapportering och har strängare tidsramar och mer detaljerade rapporteringskrav för att effektivisera hanteringen av cybersäkerhets hot. Dessutom specificerar det nya direktivet ett ramverk för sanktioner och kräver att medlemsstaterna inför effektiva straff för överträdelser, vilket bidrar till en mer enhetlig tillämpning av cybersäkerhetsåtgärder inom EU.

Tillsyn och internationellt samarbete
De nationella tillsynsmyndigheternas roll och befogenheter har stärkts markant med ytterligare befogenheter att utföra säkerhetsrevisioner, inspektioner och utfärda sanktioner. Det gränsöverskridande samarbetet och informationsutbytet mellan medlemsstaterna har också förstärkts, vilket syftar till att effektivisera EU:s respons på cybersäkerhetshot.

Säkerhetsåtgärder
NIS 2 kräver även mer omfattande tekniska och organisatoriska åtgärder för riskhantering, inklusive hantering av risker i leveranskedjan, vilket stärker skyddet mot cybersäkerhetshot.



Förbereda organisationen för NIS 2

Systematik och ständig förbättring är nyckelfaktorer för att kunna säkerställa en hög nivå av informations- och cybersäkerhet över tid. I den bemärkelsen är den internationella standarden ISO 27001 ett effektivt verktyg för att säkerställa efterlevnad av kraven i NIS 2 genom att införa ett riskbaserat, systematiskt informations- och cybersäkerhetsarbete. ISO 27001 ger ett beprövat ramverk för att etablera, implementera, underhålla och kontinuerligt förbättra ett ledningssystem för informationssäkerhet (ISMS). Här nedan presenteras några av de sätt på vilka ISO 27001 stödjer efterlevnaden av NIS 2:

- **Strategisk informations- och cybersäkerhetsplan**
  Med utgångspunkt i den initiala riskanalysen bör organisationerna utveckla en strategisk informations- och cybersäkerhetsplan som tar hänsyn till identifierade brister och sätter tydliga mål för att uppnå efterlevnad. Planen bör omfatta utveckling och implementering av riktlinjer och procedurer för effektiv riskhantering, incidentrapportering, och återhämtning efter cyberincidenter.

- **Säkerhetsåtgärder**
  För att stärka skyddet ytterligare, är det viktigt att organisationer implementerar eller förbättrar tekniska och organisatoriska säkerhetsåtgärder. Detta inkluderar allt från brandväggar och intrångsdetekteringssystem till krypteringsteknik. På den organisatoriska sidan är det viktigt att stärka till exempel interna policyer, rutiner och åtkomstkontroller.

Medvetenhet
Utbildning och medvetenhet bland personalen är avgörande för att skapa en robust säkerhetskultur. Organisationer bör därför genomföra regelbundna utbildningsprogram och initiativ för att höja medvetenheten om informations- och cybersäkerhetsrisker och säkerställa säkra och effektiva interna arbetssätt.

Leverantörshantering
En annan nyckelfaktor i förberedelserna är hanteringen av leverantörskedjan. Organisationer behöver bedöma sina leverantörers cybersäkerhetsrisker och säkerställa att de uppfyller nödvändiga säkerhetsstandarder. Detta kan innebära att genomföra revisioner och sårbarhetstester samt uppdatera befintliga kontrakt för att inkludera specifika säkerhets- och rapporteringskrav.

Incidentberedskap
För att effektivt kunna hantera säkerhetsincidenter är det kritiskt att ha uppdaterade och praktiska incidenthanterings- och återhämtningsplaner. Dessa planer bör regelbundet testas genom simuleringar och övningar för att säkerställa att organisationen är väl förberedd på potentiella cyberhot.

Samarbete och informationsdelning
Utökat samarbete och informationsdelning med andra organisationer och myndigheter är en viktig del av förberedelserna. Genom att delta i relevanta säkerhetsnätverk och initiativ kan organisationer utbyta värdefull information om hot och sårbarheter.

Revision och granskning
Slutligen är kontinuerlig övervakning och regelbundna säkerhetsrevisioner nödvändiga för att upprätthålla en hög säkerhetsnivå och anpassa sig till nya hot och utvecklingar inom cybersäkerhet.

Huvudsakliga källor

Europeiska kommissionens officiella webbplats:
https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-nis-directive

EUR-Lex:
https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=-CELEX%3A32016L1148

Regeringskansliet:
Nationell strategi för samhällets informations- och cybersäkerhet - Regeringen.se

International Organization for Standardization (IDSO) – ISO 27001:2022 och tillhörande vägledningar:
ISO - International Organization for Standardization

Bilaga 1 -
Jämförelse mellan NIS och NIS 2

	NIS	NIS 2
Tillämpningsområde	Fokuserar på leverantörer av samhällsviktiga tjänster inom energi, transport, bankväsen, hälsosektorn, och leverantörer av digitala tjänster som molntjänster, sökmotorer och online-marknadsplatser.	Utvidgar tillämpningsområdet betydligt genom att inkludera fler sektorer och typer av organisationer, såsom offentlig förvaltning, livsmedelssektor, tillverkningsindustri avseende kritiska produkter, och digitala leverantörer som sociala nätverk.
Säkerhetskrav och incidentrapportering	Kräver att berörda enheter vidtar lämpliga tekniska och organisatoriska åtgärder för att hantera cybersäkerhetsrisker och rapportera allvarliga incidenter till nationella myndigheter.	Inför strängare krav på riskhantering och rapportering av incidenter, med tydligare definitioner av vilka incidenter som ska rapporteras, samt kortare tidsramar för rapportering.
Sanktioner och efterlevnad	Uppmanar medlemsstaterna att fastställa regler om sanktioner vid överträdelser, men lämnar mycket till nationell lagstiftning.	Specificerar ett ramverk för sanktioner och kräver att medlemsstaterna inför effektiva, proportionella och avskräckande sanktioner.
Tillsyn och befogenheter	Ger nationella myndigheter befogenhet att övervaka efterlevnaden och hantera incidentrapporter, men med varierande grad av befogenheter och resurser mellan olika länder.	Stärker de nationella tillsynsmyndigheternas befogenheter och resurser betydligt, inklusive möjligheten att utföra säkerhetsrevisioner, inspektioner och att utfärda sanktioner.
Gränsöverskridande samarbete	Inrättade ett samarbetsnätverk för att främja informationsutbyte och samarbete mellan medlemsstaterna.	Förstärker detta nätverk och inför ytterligare mekanismer för gränsöverskridande samarbete och informationsutbyte, samt etablerar en mer strukturerad samarbetsgrupp.
Riskhantering och säkerhetsåtgärder	Kräver grundläggande säkerhetsåtgärder utan detaljerade specifikationer.	Specificerar mer detaljerade och omfattande krav på tekniska och organisatoriska åtgärder för riskhantering, inklusive aspekter av leveranskedjans säkerhet.
Omfattning av digitala tjänster	Inriktad huvudsakligen på vissa typer av digitala tjänsteleverantörer.	Utvidgar definitionen av digitala tjänster och inkluderar fler kategorier, vilket speglar det växande beroendet av digital infrastruktur och dito tjänster.

Vi hjälper organisationer att
växa och nå sin fulla potential
inom verksamhetsutveckling.

- Konsulttjänster
- IT-lösningar
- Utbildningar

www.canea.se
info@canea.se
+46 (0)10 459 00 00

CANEA