MINIGUIDE

Slik forbereder du deg til det nye NIS2-direktivet

advania

Oversikt over NIS2

Formål

NIS2-direktivet (Network and Information Security 2) har som mål å styrke sikkerheten og robustheten til nettverks- og informasjonssystemer over hele EU. Direktivet oppdaterer og utvider det opprinnelige NIS-direktivet for å møte de stadig voksende cybertruslene og øke beskyttelsen av kritiske infrastrukturer.

Omfang

NIS2 gjelder for et bredt spekter av sektorer og aktører, inkludert:

- Operatører av essensielle tjenester (f.eks. energi, transport, bankvirksomhet, helse, vannforsyning).
- Digitale tjenestetilbydere (f.eks. nettbaserte markedsplasser, søkemotorer, skytjenester).

Viktige datoer

- Implementering og samsvar kreves innen 18. oktober 2024.
- Regelmessig revisjon og oppdatering av sikkerhetsforanstaltninger anbefales.

Nøkkelkrav

For å oppfylle NIS2-kravene må organisasjoner implementere følgende tiltak:

Tiltak for styring av cybersikkerhetsrisiko

- Gjennomfør regelmessige risikovurderinger for å identifisere og prioritere cybersikkerhetsrisikoer.
- Utvikle og implementere omfattende sikkerhetspolicyer og prosedyrer.
- Sikre kontinuerlig overvåking og evaluering av sikkerhetstiltak.

Rapporteringsplikter

- Rapportere betydelige hendelser og sikkerhetsbrudd til relevante myndigheter innen spesifiserte tidsfrister (vanligvis innen 24-72 timer avhengig av hendelsens alvorlighetsgrad).
- Etablere klare protokoller for hendelseshåndtering og rapportering.

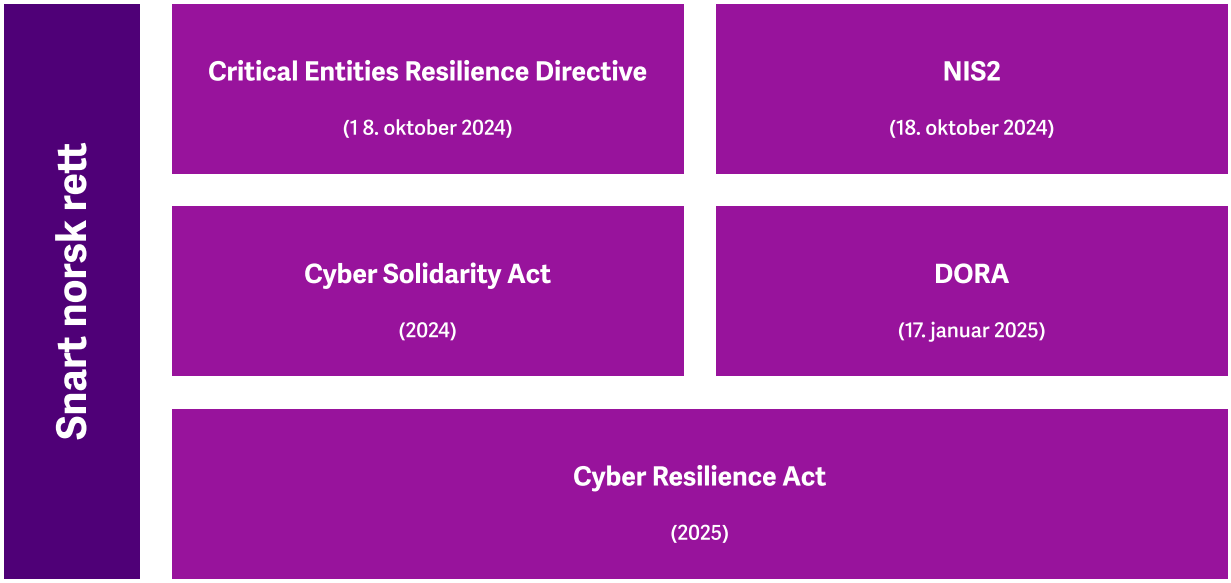
Sikkerhet i forsyningskjeden

- Sikre at alle leverandører og tjenestetilbydere oppfyller nødvendige sikkerhetskrav.
- Utføre regelmessige sikkerhetsvurderinger og revisjoner av forsyningskjeden.

Bruk av kryptografi

- Implementere kryptering og andre kryptografiske tiltak for å beskytte sensitive data, både under lagring og i overføring.
- Sørg for sikker nøkkelhåndtering og oppdatering av kryptografiske protokoller.

Flere nye lover og direktiver



Landskapet for cybersikkerhet er i endring, og lovverket må følge med. Det er flere relevante lover og direktiver som trer i kraft i nær fremtid.

Critical Entities Resilience Directive (18. oktober 2024)

- **Definisjon:** Dette direktivet fokuserer på å styrke robustheten og motstandsdyktigheten til kritiske infrastrukturer mot fysiske og digitale trusler.
- **Formål:** Beskytte essensielle tjenester som energi, transport og helse mot ulike typer risikoer, inkludert cyberangrep.

NIS2 (18. oktober 2024)

- **Definisjon:** Oppdatering av det opprinnelige NIS-direktivet for å forbedre cybersikkerheten i nettverks- og informasjonssystemer innen EU.
- **Formål:** Øke beskyttelsen mot cybertrusler for kritiske sektorer og digitale tjenester.

Cyber Solidarity Act (2024)

- **Definisjon:** Et lovforslag som fokuserer på å forbedre samarbeidet og støtten mellom EU-landene ved store cyberangrep.

- **Formål:** Fremme solidaritet og gjensidig bistand i tilfelle av omfattende cyberhendelser.

DORA (17. januar 2025)

- **Definisjon:** Digital Operational Resilience Act (DORA) har som mål å styrke den digitale operasjonelle motstandsdyktigheten til finansielle tjenester.
- **Formål:** Sikre at finanssektoren er i stand til å motstå, respondere på og gjenopprette fra cyberangrep og andre driftsforstyrrelser.

Cyber Resilience Act (2025)

- **Definisjon:** En kommende lov som har til hensikt å øke cybersikkerheten for produkter med digitale elementer.
- **Formål:** En kommende lov som har til hensikt å øke cybersikkerheten for produkter med digitale elementer.

Disse direktivene og lovene vil snart bli en del av norsk rettspraksis og vil ha stor innvirkning på hvordan organisasjoner må forholde seg til cybersikkerhet. Det er viktig å være klar over disse endringene og forberede nødvendige tiltak for å sikre samsvar.

Trinn for samsvar

For å oppnå samsvar med NIS2-direktivet bør organisasjoner følge disse trinnene:

Utfør en risikovurdering

- Identifiser og klassifiser kritiske eiendeler og systemer.
- Vurder potensielle trusler og sårbarheter.
- Prioriter risikoer basert på deres potensielle innvirkning på virksomheten.

Utvikle og implementere sikkerhetspolicyer og prosedyrer

- Etabler retningslinjer for tilgangskontroll, datasikkerhet, og nettverkssikkerhet.
- Inkluder prosedyrer for sikkerhetshendelser, katastrofegjenoppretting, og kontinuitetsplanlegging.

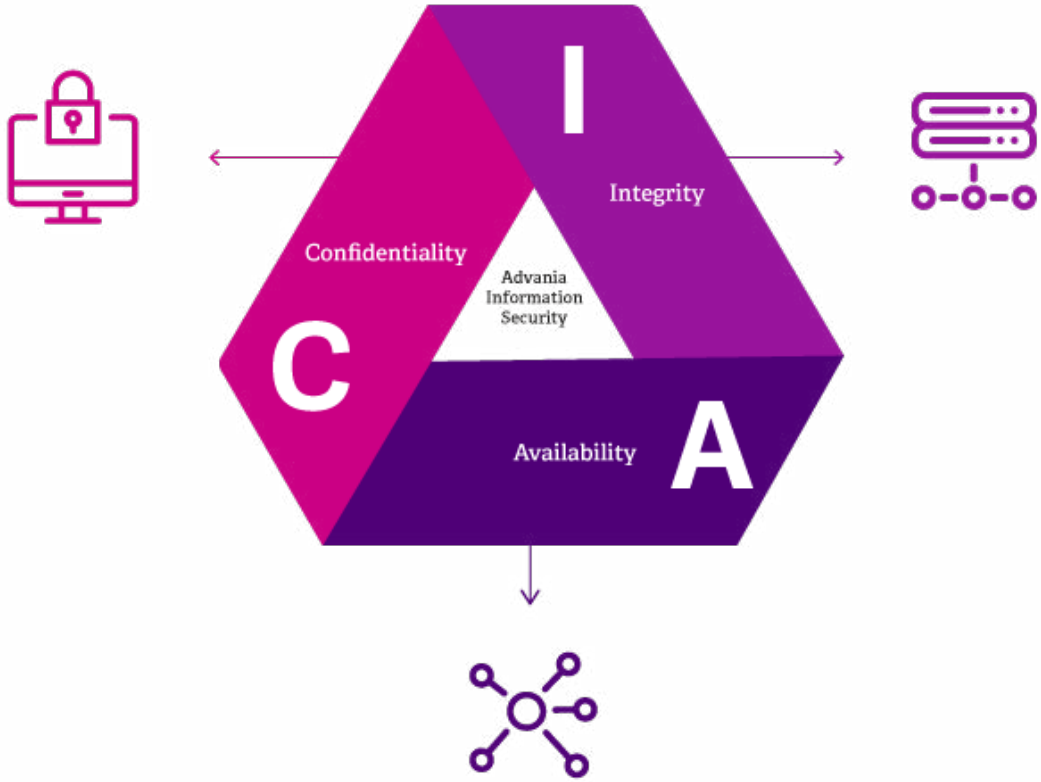
Etabler protokoller for hendelseshåndtering og rapportering

- Definer klare trinn for identifisering, rapportering, og håndtering av sikkerhetshendelser.
- Sørg for at alle ansatte er opplært i hendelseshåndteringsprosedyrer.

Gjennomgå og oppdater sikkerhetstiltak regelmessig

- Utfør regelmessige sikkerhetsrevisjoner og vurderinger for å sikre at tiltakene er effektive.
- Oppdater sikkerhetspolicyer og prosedyrer basert på nye trusler og teknologiske fremskritt.

Integritet, konfidensialitet og tilgjengelighet



Integritet, konfidensialitet og tilgjengelighet er tre grunnleggende prinsipper for informasjonssikkerhet. Figuren illustrerer hvordan disse tre prinsippene overlapper og er avhengige av hverandre for å sikre helhetlig beskyttelse av data og systemer.

Integritet (Integrity)

- **Definisjon:** Evnen til å sikre at et system og dets data ikke har blitt endret eller manipulert av uautoriserte aktører.

- **Tiltak:** Beskytter data, operativsystemer, applikasjoner og maskinvare mot uautorisert modifikasjon. Dette kan inkludere bruk av digitale signaturer, sjekksummer, og tilgangskontroller for å verifisere at data ikke er blitt tuklet med.

Konfidensialitet (Confidentiality)

- **Definisjon:** Sikrer at data kun er tilgjengelig for autoriserte brukere, systemer eller prosesser.
- **Tiltak:** Bruk av kryptering, tilgangskontroller og autentisering for å beskytte data mot uautorisert tilgang. Dette sikrer at sensitive opplysninger forblir private og kun tilgjengelige for dem som har riktig autorisasjon.

Tilgjengelighet (Availability)

- **Definisjon:** Sikrer at systemer, applikasjoner og data er tilgjengelige for brukere når de trenger dem.
- **Tiltak:** Bruk av redundans, katastrofegjenoppretting, og sikkerhetskopiering for å sikre at tjenester forblir operative selv under angrep eller tekniske feil. Dette inkluderer også tiltak for å opprettholde tjenestetilgjengelighet under DDoS-angrep (Distributed Denial of Service).

Sjekkliste: Tiltak for styring av cybersikkerhetsrisiko

For å sikre at organisasjonen din er i samsvar med NIS2, bruk følgende sjekkliste:

Identifisere kritiske eiendeler

- Opprett en liste over alle kritiske eiendeler og klassifiser dem basert på viktighet.
- Utfør en kartlegging av nettverket og identifiser alle tilkoblede enheter og systemer.

Vurder risikoer

- Bruk anerkjente risikovurderingsmetoder for å identifisere potensielle trusler og sårbarheter.
- Dokumenter alle identifiserte risikoer og deres potensielle innvirkning.

Implementere sikkerhetstiltak

- Utvikle og håndhev sikkerhetspolicyer og prosedyrer.
- Distribuer tekniske kontroller som brannmurer, kryptering, og tilgangskontroller.
- Implementer overvåkingssystemer for å oppdage og respondere på sikkerhetshendelser i sanntid.

Overvåke og gjennomgå

- Utfør regelmessige sikkerhetsrevisjoner og vurderinger.
- Gjennomgå og oppdater planen for hendelseshåndtering.
- Opplær ansatte i cybersikkerhetspraksis og hendelsesrapportering.
- Opprett en kontinuerlig forbedringsprosess for å sikre at sikkerhetstiltakene er oppdaterte og effektive.

NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY!

Se opptak av vårt seminar om NIS2-direktivet.

Tidligere i år holdt Advania, Microsoft og advokatfirmaet Brækhus et fullbooket seminar om forberedelse til NIS2. Nå har vi gjort opptakene tilgjengelig som "webinar on demand".

Du lærer mer om:

- Hva det innebærer å innføre et sikkerhetsrammeverk
- Hvordan kravene i NIS2 kan løses ved hjelp av teknologi
- Compliance-strategier etter NIS2 og DORA

Se webinar her

advania

The tech company
with people at heart

advania.no