TRUSTWORKS

RETHINKING IT AND BUSINESS

BESKYT DIN ORGANISATION OG STYRK JERES CYBERSIKKERHED MED NIS2

AF IDA HUPFELD & NIKLAS RENDBOE

Cybersikkerhed er blevet afgørende i vores hverdag pga. de store konsekvenser, som cyberangreb kan have.

Det overordnede formål med NIS2 (Network and Information Security Directive 2) er at forbedre cybersikkerheden i EU ved at stille krav til beskyttelsen af digitale tjenester og produkter, som har samfundsmæssig betydning."

TRUSTWORKS

RETHINKING IT AND BUSINESS

INTRODUKTION

I en tid hvor teknologi spiller en stadig større rolle i vores hverdag, er cybersikkerhed blevet en altafgørende faktor og risiko for både organisationer og enkeltpersoner. De seneste år har vist, at cyberangreb kan have store konsekvenser for de berørte enheder, herunder tab af data, finansielle tab og forringet omdømme. Derfor er det vigtigere end nogensinde før at beskytte vores digitale systemer mod cybertrusler.

NIS2 har til formål at sikre, at den stærkt stigende digitalisering af samfundet omfattes af tilstrækkelig sikkerhed med henblik på at forbedre det indre markeds funktioner i den Europæiske Union (EU). Formålet er altså på samfundsmæssigt plan, og skal bidrage til at sikre samfundets, og dermed vores alles, interesser.

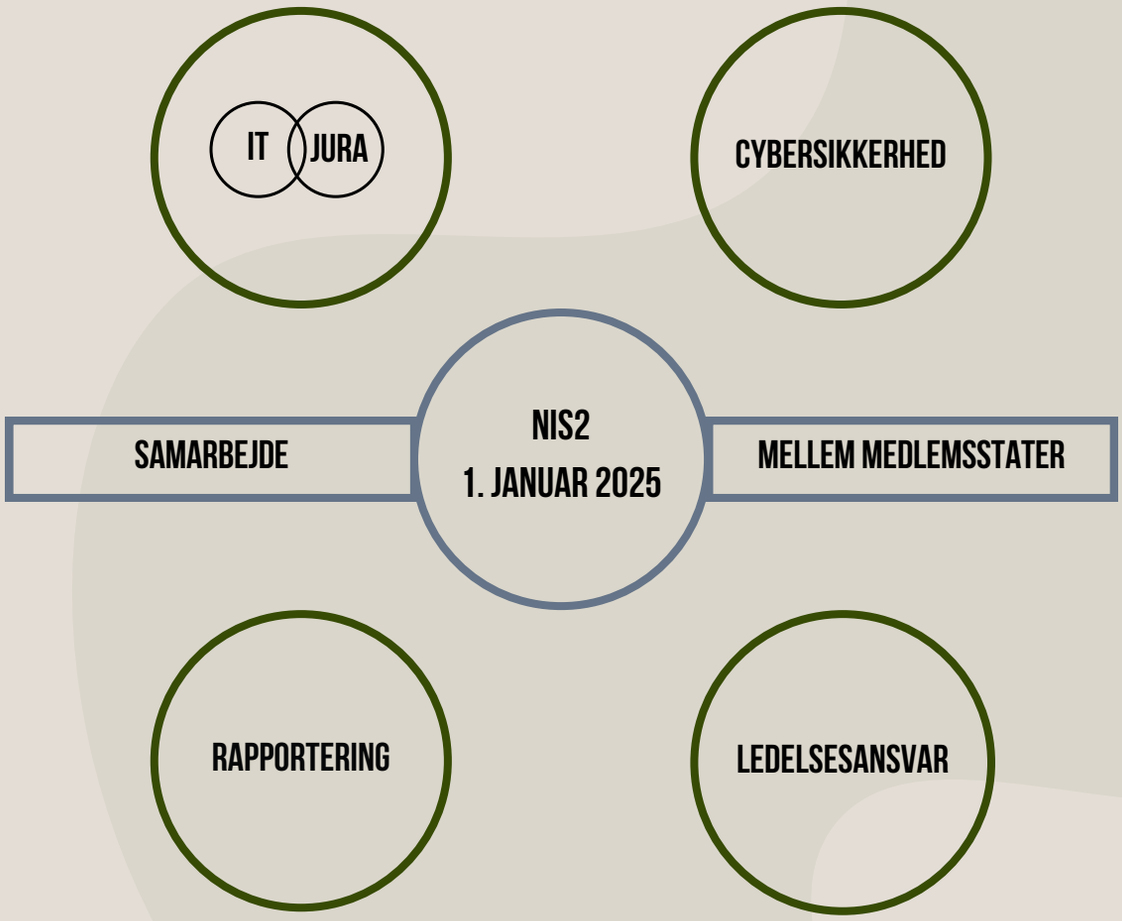
HVAD ER NIS2?

NIS2 er en opdateret version af det oprindelige NIS-direktiv fra 2016, der blev vedtaget for at styrke EU's cybersikkerhed (herunder de enkelte medlemsstaters) samt i sidste ende for at beskytte EU-borgernes digitale rettigheder og friheder. Det overordnede formål med direktivet er at forbedre cybersikkerheden i EU ved at stille krav til beskyttelsen af digitale tjenester og produkter, som har samfundsmæssig betydning.

NIS2 vedrører både stater, myndigheder og virksomheder, som spiller en samfundsvigtig rolle, og direktivet pålægger dem at anlægge en risikobaseret tilgang til cybersikkerhed.

NIS2 er et direktiv og ikke en forordning, som f.eks. GDPR. Det betyder, at dokumentet stiller generelle krav, som EUs medlemsstater derefter definerer nærmere i hver deres nationale lovgivning.

I Danmark forventes NIS2 at være gældende fra 1. januar 2025, hvor det vil være defineret gennem love og bekendtgørelser fra Forsvarsministeriet, Ministeriet for Samfundssikkerhed og Beredskab, der har det overordnede ansvar for loven i Danmark samt de ministerier og styrelser, der har ansvaret for de forskellige sektorer, der omfattes af direktivet.



HVAD ER NYT?

SKÆRPEDE SIKKERHEDSKRAV

Stiller skærpede sikkerhedskrav til risikovurderinger, implementering af sikkerhedsforanstaltninger og etablering af krisestyringsplaner.

STÆRKERE KONTROL OG HÅNDHÆVELSE

Giver udvidet adgang til stærkere kontrol og håndhævelse, herunder inspektioner og kontroller samt forøget mulighed for sanktioner og bøder. Som en tilføjelse i NIS2 kan ledelsen blive holdt personligt ansvarlige for lovbrud.

UDVIDER ANVENDELSESOMRÅDET

Udvider anvendelsesområdet for reglerne til at omfatte en bredere vifte af organisationer, herunder digitale platforme, cloud-tjenester og online markedspladser.

UDVIDET KRAV TIL RAPPORTERING

Stiller strengere krav til rapportering ved sikkerhedsbrud.

FORSYNINGSKÆDESIKKERHED

Indfører krav om at sikre passende tekniske, operationelle og organisatoriske foranstaltninger, som også gælder de omfattedes organisationers direkte leverandører og tjenesteudbydere (*forsyningskædesikkerhed*).

NIS2 øger samarbejdet mellem medlemsstaterne og opretter et netværk af forbindelsesvirksomheder for cyberkriser.

HVEM ER OMFATTET AF NIS2?

NIS2 omfatter en bred vifte af organisationer (offentlige og private), der leverer digitale tjenester og produkter i EU, herunder digitale serviceudbydere, offentlige myndigheder, transportsektoren, sundhedssektoren og finansielle tjenesteydere. Som udgangspunkt kræver det, at jeres organisation beskæftiger mere end 50 personer **OG** har en årlig omsætning eller balance på mere end 10 mio. euro samt er omfattet af nedenstående sektorer.

> 50 ANSATTE & > 10 MIO. € ÅRLIG OMSÆTNING ELLER BALANCE

NEJ → Virksomheder der er, eller ønsker at blive, leverandør til en enhed omfattet af NIS2, kan blive pålagt visse krav

JA ↓

OMFATTEDE SEKTORER:

SÆRLIG KRITISK BETYDNING

- ENERGI
- TRANSPORT
- BANK
- SPILDEVAND
- DIGITAL INFRASTRUKTUR
- IKT-TJENESTER B2B
- FINANSIEL MARKEDS-INFRASTRUKTUR
- SUNDHED
- DRIKKEVAND
- OFFENTLIG FORVALTNING
- RUMMET

ANDRE KRITISKE SEKTORER

- POST- OG KURERERTJENESTER
- AFFALDSHÅNDTERING
- KEMIKALIER
- FØDEVARER
- FORSKNING
- DIGITALE UDBYDERE
- FREMSTILLING (BL.A. MEDICINSK- OG ELEKTRONISK UDSTYR)

HVAD KRÆVER NIS2 AF DE OMFATTEDE ORGANISATIONER?

NIS2 kræver, at alle berørte organisationer skal træffe foranstaltninger for at sikre deres netværks- og informationssystemer samt rapportere om alvorlige sikkerhedsbrud til de nationale myndigheder. Det betyder, at organisationerne skal have en strategi og en handlingsplan for cybersikkerhed på plads og regelmæssigt gennemføre risikovurderinger og test af sikkerheden.

RAPPORTERING:

NIS2 stiller en række rapporteringskrav, udover at der skal sendes meddelelse til modtagerne af en tjeneste ved et væsentligt "incident". Denne rapportering skal indgives til Computer Security Incident Response Team (CSIRT'en) eller den kompetente myndighed.

KRAV TIL RAPPORTERING:

24 TIMER	72 TIMER	ÉN MÅNED
Uden unødigt ophold og senest inden for 24 timer.	Uden unødigt ophold og senest inden for 72 timer.	Endelig rapport.
Indhold: Tidlig varsel om et væsentligt "incident".	Indhold: "Incident" underretning, herunder indledende vurdering af alvoren og indvirkningen.	Indhold: • Beskrivelse af "incidents" samt alvor og indvirkning. • Type af trussel eller grundlæggende årsag. • Anvendte og igangværende afbødende foranstaltninger. • Evt. grænseoverskridende virkninger.

MINIMUMSFORANSTALTNINGER:

Der er fortsat i NIS2 krav om, at der skal træffes passende og forholdsmæssige tekniske og organisatoriske sikkerhedsforanstaltninger, som skal sikre beskyttelse af net- og informationssystemer, herunder disses fysiske miljøer mod "incidents".

I forhold til direktivets forgænger, er NIS2-kravene blevet udvidet og omfatter nu som minimum:

1. Politikker for risikoanalyse og informationssystemsikkerhed.
2. Håndtering af "incidents".
3. Driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring.
4. Forsyningskædesikkerhed (forholdene til direkte leverandører eller tjenesteudbydere).
5. Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer.
6. Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.
7. Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.
8. Politikker og procedurer for kryptografi og kryptering.
9. Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.
10. Brug af sikre løsninger for interne kommunikationssystemer.

HVORDAN KAN NIS2 HJÆLPE DIN ORGANISATION?

NIS2 kan bidrage til at forbedre en række områder i jeres organisation udover at sikre overholdelse af lovgivningen og dermed at undgå eventuelle sanktioner. Eksempler på dette inkluderer:

BEDRE RISIKOSTYRING

Øget fokus på risikostyring kan bidrage til hurtigere at identificere potentielle trusler og sårbarheder og dermed gøre organisationen i stand til at foretage proaktive foranstaltninger. En stærk sikkerhedsprofil kan bidrage til at opbygge tillid hos kunder og samarbejdspartnere og øge organisationens omdømme.

STYRKET SIKKERHED

Ved at implementere sikkerhedsforanstaltningerne omfattet i NIS2 kan organisationens kritiske infrastruktur beskyttes bedre mod cyberangreb, som kan føre til tab af data og beskadiget systemer.

BEDRE INCIDENT MANAGEMENT

Procedurer til håndtering af ”incidents” kan bidrage til, at organisationen kan reagere hurtigt på et “incident” og mindske dets påvirkning på organisationen. Dette kan også hjælpe med at begrænse skadevirkningen for kunder og samarbejdspartnere og opretholde deres tillid. Effektiv håndtering af “incidents” kan derudover føre til mindre økonomisk tab og kortere tid til genopretning, hvilket gavner organisationen på både kort og lang sigt.

KONKURRENCE-FORDEL SOM LEVERANDØR

Som en del af NIS2 stilles der krav om forsyningskædesikkerhed, hvilket betyder, at det ikke er nok kun at have styr på den interne sikkerhed. Det skal derimod også sikres, at direkte leverandører til de omfattede organisationer efterlever et tilstrækkeligt sikkerhedsniveau. Ved at have tidligt fokus på NIS2 som leverandør, kan der derved opnås en konkurrencefordel.

ANBEFALING

NIS2 kræver fokus på tværgående forankring, som kan være yderst tids- og ressourcekrævende. Vi anbefaler følgende proces som forberedelse:

1. AFKLARING: OMFATTET AF NIS2

- Kritiske sektorer
- Leverandørstatus
- Gap-analyse

2. IDENTIFIKATION: DRIFTSKRITISKE AKTIVER

- Systemer
- Hardware
- Data
- Infrastruktur

3. RISIKOVURDERING: FORRETNINGSPROCESSER

- Intern/ekstern trusler
- Sandsynlighed
- Konsekvenser
- Prioritering

4. IMPLEMENTERING: SIKKERHEDSFORANSTALTNINGER

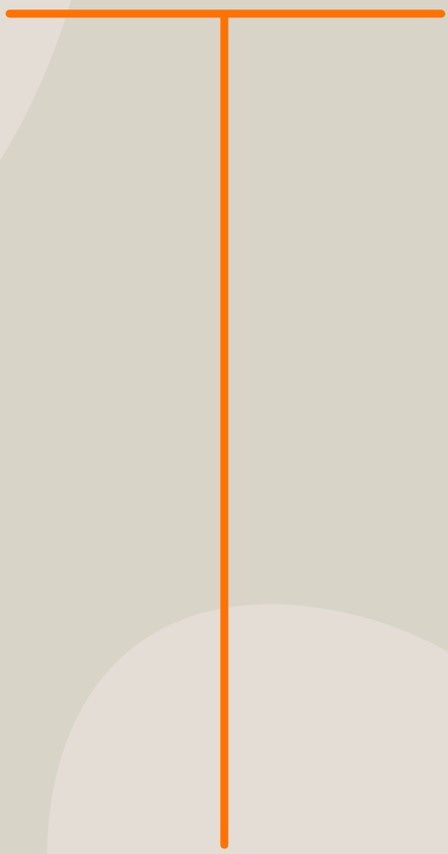
- Tekniske løsninger
- Organisatoriske tiltag
- Træning og awareness
- Langsigtede planer

5. OVERVÅGNING: RAPPORTERING OG RESPONS

- Systemer til detektering
- Hændelsesrapportering
- Onboarding af medarbejdere
- Løbende evaluering

- Hvis I er omfattet af NIS2, bør I starte med at identificere driftskritiske aktiver, herunder software, hardware, data og infrastruktur, der er afgørende for virksomhedens daglige drift og levere værdi til kunderne.
- Dernæst bør organisationen lave en risikovurdering af forretningsprocesserne og prioritere sikkerhedsinitiativer og ressourcer mod de processer, der udgør de største risici for organisationen.
- Efter at have identificeret og vurderet aktiver og forretningsprocesser skal organisationen udarbejde en plan for implementering og vedligeholdelse af passende sikkerhedsforanstaltninger. Det er også vigtigt at have systemer og planer på plads for overvågning og rapportering af hændelser.
- Endelig anbefales det, at organisationer arbejder med cybersikkerhed i en cirkulær proces og forholder sig proaktivt til trusselsbilledet.

Trustworks er en IT-transformationspartner, der skaber resultater i store og krævende digitale initiativer. Vi har omfattende erfaring med at levere strategisk udvikling og digitalisering inden for grøn omstilling, finans, offentlig digitalisering og Pharma & Life Science.
Vi er en end-to-end partner fra idé til omstilling og implementering. Vores specialer er IT-arkitektur, forretningsanalyse, projektledelse, applikationsmodernisering, integrationer, cybersikkerhed og systemudvikling.



TRUSTWORKS

RETHINKING IT AND BUSINESS