
S&CO
Salamon&Company

Salamon&Company

Benjamin Salamon

Partner og konsulent
Mail: Benjamin@salamon.dk
Tele: 4061 6828

Michael Gadgaard

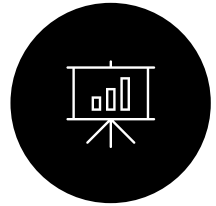
Partner og konsulent
Mail: Michael@salamon.dk
Tele: 5354 5334

Dagens Agenda

- NIS2 – Lovgivningshistorik
- Kort om NIS2
- Hvem er omfattet af NIS2?
- NIS2 nøgleelementer
- Risikohåndtering
- Hvordan kommer man i gang?
- Forsyningskædesikkerhed
- Underretningspligt
- Sanktioner
- Afrunding og spørgsmål

NIS2 lovgivningshistorik

- Fra direktiv til dansk lovgivning

Forslag til NIS2 direktiv fremsat	Politisk aftale om NIS2	Offentliggørelse af endeligt vedtaget NIS2 i EU-tidende	NIS2 ikrafttræden	Implementering i dansk lovgivning
				
December 2020	Maj 2022	27. december 2022	16. januar 2023	18. oktober 2024

Salamon&Company

Kort om NIS2

NIS2

Direktivet om netværks- og informationssikkerhed (Network & Information Security).

De enkelte medlemslande skal have det implementeret inden for 21 måneder
(Nu 17 måneder).

- Hvad er NIS2 Direktivet
- Årsagen til NIS2
- Formålet med NIS2
- Hvorfor er NIS2 vigtig?

Minimumsharmonisering

Medlemsstaterne kan vedtage eller opretholde bestemmelser, der sikrer et højere cybersikkerhedsniveau.

Hvorfor er det vigtigt også i en dansk kontekst?

DR

POLITIK

Efterretningstjeneste oplever stor trussel: Cybe-rangreb kan lægge samfundet ned

Truslen for omfattende cyberangreb på energisektoren i Danmark er på sit højeste niveau, vurderer FE.

- 48 succesfulde cyberangreb mod den europæiske forsynings- og energisektor siden 2015, heraf er 20 angreb er fra 2022.
- 6 ud af de 48 angreb har ramt danske virksomheder.
- 15 angreb har påvirket OT-netværket

Kilde: Cyberangreb mod europæiske energi- og forsyningsselskaber, EnergiCert, september 2022.

Salamon&Company

NIS2 bliver håndhævet om kun…

17 Måneder

18. oktober 2024

De ondsindede trusler venter dog ikke på denne dato – Gør I?

Hvem er omfattet af NIS2?

Væsentlige enheder

- er omfattet af direktivets bilag I.
- er underlagt mere omfattende forpligtelser end vigtige enheder.

Salamon&Company

Hvem er omfattet af NIS2?

Vigtige enheder

- er omfattet af direktivets bilag II.
- er underlagt mindre omfattende forpligtelser end væsentlige enheder.

Salamon&Company

Undtagelsesbestemmelse

- Mikro og små virksomheder er som udgangspunkt undtaget
- Der er dermed krav om mindst 50 ansatte og en årlig omsætning eller en årlig balance på over 10 mio. EUR.

Undtagelse til undtagelsesbestemmelsen

Inden for en række sektorer vil også mikro og små virksomheder være omfattet af NIS2, herunder eksempelvis:

- Udbyder af offentlige elektronisk kommunikationsnet
- Enheder, der er den eneste udbyder af en tjeneste, der er væsentlig for opretholdsen af kritiske samfundsmæssige eller økonomiske aktiviteter
- Enheder, der er kritiske pga. deres specifikke betydning på regionalt eller nationalt plan for en given sektor eller type af tjeneste.

NIS2 - Nøgleelementer

Risikostyring

Ledelsesmæssig forankring

Politikker, processer og procedurer

Uddannelse

Hændelseshåndtering og rapportering

Kontrol og løbende monitorering

Forebyggelse

Håndhævelse - sanktionsmuligheder

Salamon&Company

NIS2 – Sikkerhedsforanstaltninger
- Risikobaseret tilgang

- Omfattende organisationer skal træffe passende og forholdsmæssige *tekniske, operationelle og organisatoriske sikkerhedsforanstaltninger*.
    - De skal styre risiciene for sikkerheden i net og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester.
    - De skal forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester.
- Ved vurdering af proportionaliteten af disse foranstaltninger tages der behørigt hensyn til *graden af enhedens størrelse og sandsynligheden for hændelser og deres alvor*, herunder deres *samfundsmæssige og økonomiske indvirkning*.

Risikovurderinger

Informationssikkerhed

Udgangspunkt i organisationen

GDPR

Udgangspunkt I datasubjekterne

NIS2

Udgangspunkt i samfundet

Risikohåndteringstiltag

Artikel 21

1. Politikker for risikoanalyse og informationssystemsikkerhed
2. Håndtering af hændelser
3. Driftskontinuitet, herunder backup-styring. Supply chain security.
4. Forsyningskædesikkerhed
5. Sikkerhed ifbm. Erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer.
6. Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici
7. Cyber security hygiejne og uddannelse
8. Politikker og processer for kryptografi, og hvor relevant kryptering.
9. Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver (asset management)
10. Multi-factor autentifikation e.l.

Risikohåndteringstiltag – fordelt i temaer

Artikel 21

1. Politikker og procedurer

- Politikker for risikoanalyse og informationssikkerhed
- Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici
- Politikker og procedurer vedrørende brug af kryptering og hvor det er relevant, kryptering.

2. Overvågning og hændelseshåndtering

- Håndtering af hændelser
- Driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe og krisestyring.

3. Supply chain og applikationssikkerhed

- Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere
- Sikkerhed ifbm. erhvervelse, udvikling og vedligeholdelse af net- og informationssikkerhedssystemer, herunder håndtering og offentliggørelse af sårbarheder.

4. Grundlæggende sikkerhedstiltag

- Cyber security hygiejne og uddannelse
- Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver
- Brug af løsninger med multi-factor autentifikation e.l

Hvordan kommer man i gang?

Identificer om jeres virksomhed/organisation er omfattet af NIS2

Hvor skal ansvaret forankres?

Skab opmærksomhed hos topledelsen, ansvar, sanktioner og bøder

Er der behov for at revidere jeres interne politikker og processer?

10 mål for risikostyring af cybersikkerheden

Hvem skal involveres?

Projektplan og projektgruppe

Uddannelse og træning af topledelsen for at sikre indsigt i risikostyring

Vurdér cybersikkerheden i leverandørkæden

Er der behov for at revidere standardaftaler og third-party risk framework?

Hvad er allerede implementeret i din organisation?

Værktøj til at strukturere, kontrollere og styre virksomhedens håndtering af informationssikkerhed

Salamon&Company

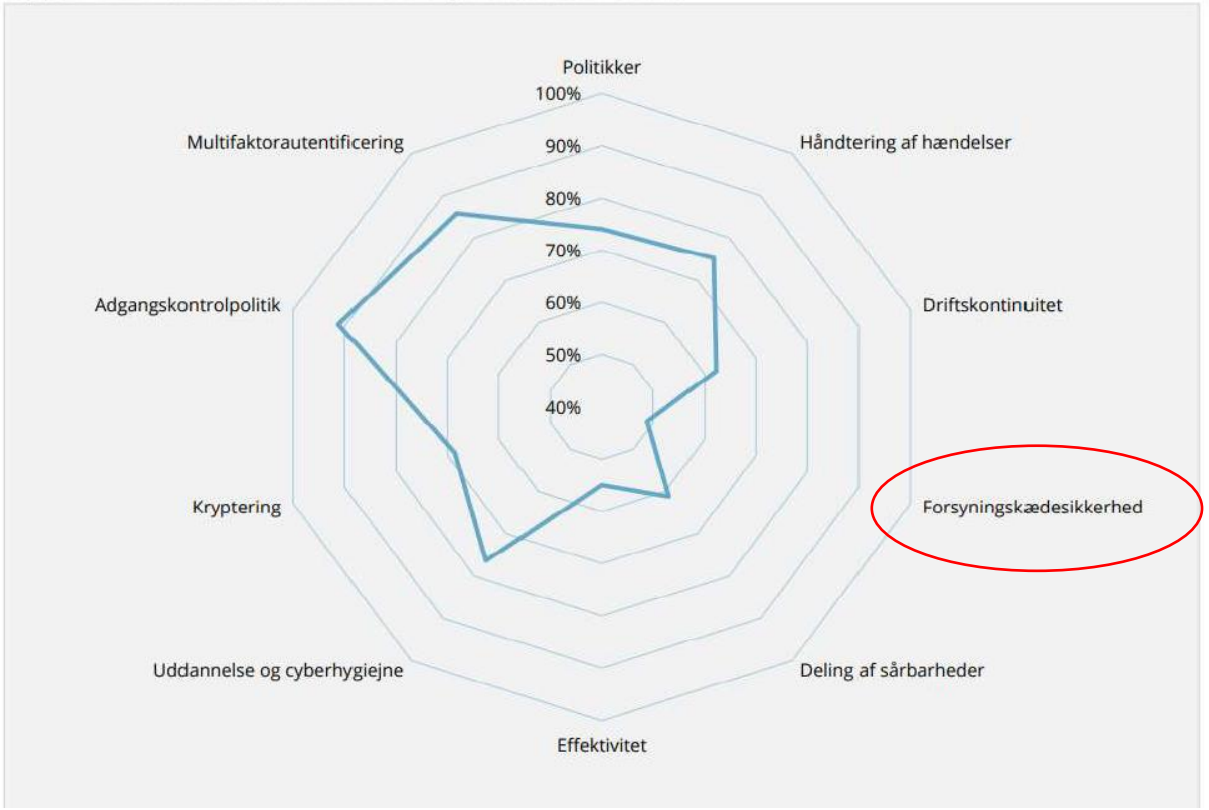
Hvilke krav er sværest at leve op til?

Rapport fra Industriens fond

Adgangskontrolpolitikker volder ikke de store problemer – MFA mv.

Forsyningskædesikkerhed og test af tiltagenes effektivitet er langt sværere

Figur 2.12 Andel af virksomheder der lever op til direktivets 10 krav



Salamon&Company

Hvad siger direktivet om forsyningssikkerhed?

Artikel 21

Foranstaltninger til styring af cybersikkerhedsrisici

1. Medlemsstaterne sikrer, at væsentlige og vigtige enheder træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester.

Under hensyntagen til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt gennemførelsesomkostningerne skal de i første afsnit omhandlede foranstaltninger tilvejebringe et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risiciene. Ved vurderingen af proportionaliteten af disse foranstaltninger tages der behørigt hensyn til graden af enhedens eksponering for risici, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning.

2. De i stk. 1 omhandlede foranstaltninger baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende:

[...]

d) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere

Cyberangreb via leverandører (Supply-chain angreb)

- Ved at kompromittere leverandører kan hackere få adgang til bredere vifte af mål.
  - Det kan samtidig være langt vanskeligere at opdage
  - Særligt interessant med angreb mod leverandører, der har direkte adgang til kunders it-systemer.
  - Denne metode anvendes ofte af statslige aktører, der er meget tålmodige i deres angreb.

Cybersikkerhedstal

Check Point vurderer i deres årlige cybersikkerhedsrapport for 2022, at

- Antallet af cyberangreb er steget med 50% siden deres årlige rapport for 2021
- De fleste cyberangreb udnytter svagheder kendt igennem flere år.
- Der udføres stadig flere cyberangreb via leverandører (supply-chain angreb)

Tredjeparts risikostyring

Dokumenter jeres tredjeparts landskab

Tilstrækkelige medarbejder-ressourcer og -kompetencer

Vurdere effektiviteten

Forankring af processen hos topledelsen

Implementér en moden tredjeparts risikohåndterings proces (CIS18 + NIST CFS eller ISO27002:2022 pkt. 5.19-22)

Salamon&Company

Forsyningskædesikkerhed og dokumentation

Forsynings-kædesikkerhed

- Det er ikke tilstrækkeligt kun at se på egen organisation
  - Leverandører
  - Sikker udvikling
- Sikre gennemførelse af tilsynsbeføjelser og hændelsesrapportering

Dokumentations krav

- At der er gennemført aktuelle risikovurderinger
- At der er implementeret sikkerhed målrettet risikoen, herunder at sikkerheden er understøttet i relevante kontrakter

Supply chain og applikationssikkerhed – konkrete tiltag

- Overblik over samtlige leverandører og digitale systemer med betydning for enhedens egen samfundskritiske leverance
- Et klassificeringssystem, hvor i man grupperer både fysiske og digitale leverandører i forhold til deres grad af kritiske leverancer
- En kontraktgennemgang af alle eksisterende leverandører for at konstatere, om sikkerhedsforanstaltninger i forhold til cybersikkerhed indgår eller ikke
- Forhandle nye kontrakter med relevante sikkerhedsforanstaltninger
- Planlægning og testning af beredskabsplaner og genopretningsplaner skal udføres med leverandører og tredjepartsudbydere.

Certificeringer og standardisering

- Medlemsstaterne tilskynder benyttelse af europæiske eller internatale standarder og specifikationer, der er relevante for sikkerheden i net- og informationssystemer (art. 25)

CIS18 / ISO27002

CIS18 kontroller – den praktiske og best practice baserede tilgang til arbejdet med cybersikkerhed

- Kan mappes til ISO27001 og ISO27002 for compliance og referencer
- Vedligeholdes løbende
- Bruges i det daglige arbejde med cybersikkerhed, men kan også indgå i udbud og kontrakter som fælles reference for kunde og leverandør

CIS Kontrol	CIS Sikrings-foranstaltninger	AktivType	Sikkerheds Funktion	Title	Beskrivelse	IG1	IG2	IG3
3	3,14	Data	Detect (Opdage)	Log ikke-autoriseret dataadgang	Logføre uautoriseret dataadgang, inklusive ændring og bortskaffelse.			
4				**Sikker konfiguration af virksomhedens aktiver og software**	***Oprette og vedligeholde den sikre konfiguration af virksomhedens aktiver (slutbrugerenheder, inklusive bærbare og mobile, netværksenheder; ikke-computende / IoT-enheder og servere) og software (operativsystemer og applikationer).***			
4	4,1	Applikationer	Protect (Beskytte)	Oprette og vedligeholde en sikker konfigurationsproces	Oprette og vedligeholde en sikker konfigurationsproces for virksomhedsaktiver (slutbrugerenheder, inklusive bærbare og mobile, ikke-computende / IoT-enheder og servere) og software (operativsystemer og applikationer). Gennemgå og opdater dokumentationen årligt, eller når der sker betydelige virksomhedsændringer, der kan påvirke denne beskyttelse.	x	x	x
4	4,2	Netværk	Protect (Beskytte)	Oprette og vedligeholde en sikker konfigurationsproces til netværksinfrastruktur	Oprette og vedligeholde en sikker konfigurationsproces for netværksenheder. Gennemgå og opdater dokumentationen årligt, eller når der sker betydelige virksomhedsændringer, der kan påvirke denne beskyttelse.	x	x	x
4	4,3	Brugere	Protect (Beskytte)	Konfigurer automatisk sessionslåsning på Enterprise-aktiver	Konfigurer automatisk sessionslåsning på virksomhedens aktiver efter en defineret periode med inaktivitet. For almindelige operativsystemer må perioden ikke overstige 15 minutter. For mobile slutbrugerenheder må perioden ikke overstige 2 minutter.	x	x	x

Salamon&Company

Implementering af NIS2 krav i nuværende aftaler

- Leverandøren vil ikke kunne blive pålagt bøder for manglende overholdelse af kravene i NIS2 (Såfremt de ikke er omfattet af reglerne).

- Det er derfor almindelig aftaleretlige krav som skal regulere forholdet mellem kunden og leverandøren.

- Leverandøren kan ikke lave en risikovurdering af sig selv – men kan evt. bistå med relevant dokumentation, test mv.

- Assistance til hændelseshåndtering

- Afgræsning af compliance ansvar
- Governance (Roller og ansvar)
- Sikkerhedsbilag
    - Beskrivelse af specifikke sikkerhedsforanstaltninger over for kunden i relation til services/produkter
    - Beskrivelse af egne sikkerhedstiltag (certificeringer, revision mv.)
    - Proaktiv tilgang til dokumentation sikrer konkurrencedygtighed
- Mappe kundens complianceansvar med leverandørens ydelser
    - Sådan skal leverandøren efterleve NIS2
    - Sådan skal leverandøren bistå med at efterleve kunden med NIS2

Implementering af NIS2 krav i nuværende aftaler

- Status for nuværende sikkerhedsbilag

- Risikostyring
  - Er der noget anvendelig risikostyrings og identifikationsmateriale

- Regulatorisk compliance/lovmedholdelighed
  - Hvad kan der presses ind som almindelig regulatorisk compliance
  - Hvem har identifikations, analyse ansvaret
  - Betalbar/ikke-betalbar ydelser

- Omfang af ændringer
  - Genforhandling
  - Brede compliance klausuler (herunder complinace med kundespecifik lovgivning)
- Er der udbudsretligt råderum for ændringer eller kræver det genudbud
  - Grundlæggende ændringer af services

-

NIS2
-
Underretning

NIS2: Underretningsprocessen

Tidlig varsel

Inden for 24 timer

Underretning

Inden for 72 timer

Foreløbig rapport

På anmodning

Endelig rapport

En måned

(Efter underretningen)

Salamon&Company

Underretning- om væsentlige hændelser

- Væsentlige og vigtige enheder skal uden unødig ophold foretage underretning til CSIRT og/eller den kompetente myndighed ved enhver hændelse, der har en væsentlig indvirkning på levering af deres tjenester.

- Hvor det er relevant skal der også ske underretning til modtagerne af tjenesten.

Væsentlighedskriteriet

En hændelse anses for at være væsentlig, hvis:

- Den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenester eller økonomiske tab.
- Den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immaterielle skader.

Ledelsesmæssig forankring

Ledelsesorganerne i væsentlige og vigtige enheder forpligtes med NIS2 til at:

- Godkende foranstaltninger til styring af cybersikkerhedsrisici efter NIS2
- Føre tilsyn med implementeringen af disse risikohåndteringsforanstaltninger.

Ledelsesorganerne gøres tillige ansvarlige for manglende overholdelse af NIS2-kravene.

Uddannelse af øverste ledelse

- Medlemmer af ledelsesorganet i væsentlige og vigtige enheder skal efter NIS2 regelmæssigt følge kurser, så de opnår:

”tilstrækkelig kundskaber og færdigheder til at kunne identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici og deres indvirkning på de tjenester, leder leveres af enheden”.

NIS2 Sanktioner

- Væsentlige enheder kan pålægges administrative bøder på op til 10 mio. EUR eller op til 2% af den samlede globale årsomsætning i den virksomhed, alt efter hvad er højest.

- Vigtige enheder kan pålægges administrative bøder på op til 7 mio. EUR eller op til 1,4 % af den samlede globale årsomsætning i den virksomhed, alt efter hvad der er højest.

Opsummering

- Der indføres differentieret tilsyn ift. vigtige og væsentlige enheder
- Forsyningskædesikkerhed og risikovurderinger er vigtige – men tidskrævende
- Skærpet krav til hændelsesrapportering
- Ledelsesmæssig forankring er afgørende
- Krav til uddannelse
- Sanktioner og håndhævelse er skærpet markant

NIS2 bliver håndhævet om kun…

17 Måneder

18. oktober 2024

Salamon&Company

Tak for i dag.

Benjamin Salamon

Partner og konsulent
Mail: Benjamin@salamon.dk
Tele: 4061 6828

Michael Gadgaard

Partner og konsulent
Mail: Michael@salamon.dk
Tele: 5354 5334

Salamon&Company