



NIS-richtlijn en beveiliging van toeleveringsketen: het belangt ook u aan!

09 september 2022, 15:25

Tatiana Galibus

Al gehoord van de NIS-richtlijn? De meeste maakbedrijven zijn zich nog niet bewust van het belang van deze regelgeving in de EU. Bij Sirris volgen we de implementatie van deze richtlijn in België op de voet. De regels die erin worden vastgelegd, belangen u immers rechtstreeks als u in een van de 3000 kmo's werkt die de Belgische maakindustrie rijk is, en zelfs als u werkzaam bent voor een leverancier, een machinebouwer of een digitale dienstverlener.

Waarover gaat de richtlijn ?



(ec.europa.eu)

De NIS(-1)-richtlijn werd in 2016 door de EU goedgekeurd. Het was de eerste regelgeving inzake cyberbeveiliging op Europees niveau. In België werd de richtlijn in 2019 toegepast in de vorm van de NIS-wet. Wat zijn de verplichtingen onder de huidige NIS-richtlijn?

Lidstaten	• ontwikkeling van nationale strategieën voor cyberbeveiliging • grensoverschrijdende samenwerking • de aanbieders van essentiële diensten (AED) identificeren op het gebied van: energie, vervoer, bankwezen, infrastructuur voor de financiële markten, gezondheidszorg, drinkwater, en digitale infrastructuur.
Aanbieders van essentiële diensten	• minimale veiligheidsmaatregelen nemen • belangrijke incidenten melden
Aanbieders van essentiële digitale diensten	• voldoen aan deze vereisten inzake beveiliging en kennisgeving

Als gevolg van de toenemende cyberaanvallen en de rampzalige gevolgen ervan, stelde de EU in december 2020 NIS-2 voor. De nieuwe versie bevat onder meer de volgende verbeteringen:

- meer sectoren en entiteiten binnen het toepassingsgebied van de cyberbeveiliging
- uitgebreide beveiligingsvereisten
- persoonlijke betrokkenheid en verantwoordelijkheid van managers en bestuursraden
- strenge sancties en hogere bedragen
- gedetailleerde rapportageverplichtingen voor incidenten
- nadruk op de versterking van de beveiliging van de toeleveringsketen

De kans is groot dat u er nog niet veel van gehoord hebt, want deze regels zijn nog niet algemeen aanvaard. Verwacht wordt dat de situatie tegen 2025 niettemin zal veranderen met de goedkeuring van de Belgische NIS-wet.

Waarom is de richtlijn belangrijk?

Kort samengevat stelt de EU voor om de vereisten voor de leveranciers aan te scherpen, de sancties te verzwaren en CEO's en bestuursraden een persoonlijke verantwoordelijkheid op te leggen. De versterkte en gepersonaliseerde regelgeving zal alle bedrijven beïnvloeden die betrokken zijn bij uw interacties in de toeleveringsketen en zal onvermijdelijk veranderingen teweegbrengen in de manier waarop u met de leveranciers samenwerkt en producten aan de klanten levert. De beveiliging zal veel essentiëler worden voor de bedrijfscontinuïteit.

Voor sommigen kan dit eng klinken, maar voor wie zich al op de toekomst voorbereidt, komt dit niet als een verrassing. Cyberbeveiliging dringt zich op als toegevoegde waarde aan uw product en vroeg of laat zult u niet meer kunnen verkopen zonder deze 'feature'.

En wat als u deze veranderingen in de wetgeving negeert? Wat betekent het voor een kmo? Het betekent zeker dat u klanten zult verliezen als u niet veilig genoeg bent. De meeste bedrijven zijn betrokken bij steeds complexere en uitgebreidere interacties in de toeleveringsketen, die vaak nog niet beveiligd zijn. Als u bijvoorbeeld 'ja' antwoordt op een van de volgende vragen, betekent dit dat u in NIS-termen niet veilig bent:

- Verleent u admin-rechten aan externe medewerkers zonder de machines en het toegangscontrolebeleid te specificeren?
- Vermijdt u geregelde controles van de externe verbindingen?
- Vergeet u soms de poorten en tools voor onderhoud op afstand te controleren?

Ben ik veilig?

Helaas bestaat er geen eenduidige vragenlijst met betrekking tot de beveiliging van uw toeleveringsketen en de NIS-2-richtlijn. Sirris werkt aan een dergelijke automatische tool in het kader van het Cornet-project Cybersecurity 4.0.

Momenteel biedt Sirris maakbedrijven gratis intakes van 1 uur rond cyberbeveiliging, met focus op de toeleveringsketen. We stellen daarbij enkele vragen en suggereren oplossingen voor de mogelijk gedetecteerde kritieke kwetsbaarheden. Bent u geïnteresseerd in een dergelijke intake?

[Neem dan zeker contact met ons op!](#)

Wat nu?

Wees voorbereid. Wees hackers voor. Met het cyberbeveiligingslandschap dat voortdurend verandert, is het essentieel de vinger aan de pols te houden: nu aanvallen steeds georganiseerder worden, moet beveiliging meer op samenwerking en wendbaarheid gericht zijn. En dat betekent dat de beveiliging van de hele toeleveringsketen moet worden gewaarborgd.

Sirris organiseert een praktijkgericht opleidingstraject van 2 maanden om maakbedrijven te helpen met cyberbeveiliging. We bieden individuele coachingsessies en masterclasses bij u ter plaatse, om u te helpen uw eigen cyberbeveiligingsstrategie te ontwerpen en specifieke risico's uit de weg te ruimen.

Bekijk ons collectief en individueel aanbod [hier](#)!

Meer lectuur over dit onderwerp:

ENISA: <https://digital-strategy.ec.europa.eu/en/policies/nis-directive>

CCA Belgium: <https://www.cybersecuritycoalition.be/nis-2-where-are-you/>

Auteurs



Tatiana Galibus