NIS2: hefboom en accelerator voor cybersecurity

inetum

Cybersecurity versus Compliance

Belgische CIO's zijn zich maar al te zeer bewust van het belang van cybersecurity. Maar hoe zit dat met compliance? Vinden die CIO's het ook belangrijk om de opgelegde regelgeving rond cybersecurity zo goed mogelijk na te leven?

Het antwoord op die vraag vinden we in lokaal marktonderzoek van **Beltug**, dat met 2200 leden de grootste vereniging voor CIO's en IT-beslissingsnemers in België is.

Cybersecurity blijft 'top of mind'

In het **jaarlijkse prioriteitenonderzoek** van Beltug scoort cybersecurity al een hele tijd opvallend hoog. En hoewel je in 2023 niet om de doorbraak van artificiële intelligentie (AI) heen kon, stond ook cybersecurity dat jaar opnieuw helemaal bovenaan het prioriteitenlijstje van de Belgische CIO.

In 2023 waren liefst vier prioriteiten uit de top tien gelinkt aan cybersecurity: van het uitwerken van een strategie en een architectuur voor IT-security tot en met het bevorderen van het bewustzijn rond security en privacy bij IT-gebruikers en het plannen van de respons op cyberincidenten, inclusief de oprichting van een eigen Computer Security Incident Response Team (CSIRT). In totaal werd in 2023 zelfs bijna de helft van de top veertig van CIO-prioriteiten ingenomen door securitythema's.

> Vandaag stelt geen enkele IT-beslissingsnemer de zin van investeringen in cybersecurity nog echt in vraag.
>
> **Levi Nietvelt,**
> *Beltug*

Dat het de Belgische CIO's menens is met hun aandacht voor cybersecurity, blijkt ook uit de **tweejaarlijkse gebruikersenquête** van Beltug. Daarin blijven de investeringen in cybersecurity overduidelijk op peil. Zo verwachtte amper 3,5 procent van de bedrijven begin 2023 dat die investeringen dat jaar zouden afnemen. Een kwart verwachtte dat ze stabiel zouden blijven, terwijl bijna zeven op de tien ondervraagden (68%) hun investeringen in cybersecurity nog zagen toenemen.

Compliance niet expliciet genoemd

Kijken we naar de aandacht van de Belgische CIO's voor compliance, dan duikt een heel ander beeld op. Tenzij je onder diezelfde noemer ook termen als governance (van data, IT, AI, ...) of ESG (duurzaamheidsrapportering) wil vatten, komt het woord compliance amper voor in het prioriteitenlijstje van de Belgische CIO.

Nochtans vormt compliance vandaag al een belangrijke uitdaging, zeker op het gebied van cybersecurity en dataprivacy. Het ziet er bovendien naar uit dat die uitdaging de komende jaren alleen nog groter zal worden. Nieuwe wet- en regelgevingen, met name van de Europese Unie, volgen elkaar in sneltempo op. Dat maakt het er het niet eenvoudig op om bij te blijven. Temeer omdat de regelgevingen voor het ene land ook niet altijd in het andere land gelden.

> Aangezien compliance nauwelijks wordt genoemd in de prioriteiten van de CIO's, zou die dan 'onbelangrijk' kunnen zijn?
>
> **Levi Nietvelt,**
> *Beltug*

NIS2-compliance: de speeltijd is voorbij

Overheden, met de EU op kop, leggen bedrijven steeds meer eisen op inzake cybersecurity. Een treffend voorbeeld is NIS2, de opvolger en vervanger van de **Network and Information Security (NIS) Directive** uit 2016. Die originele versie wordt ook wel eens de allereerste cybersecuritywet genoemd. Het uiteindelijke doel van beide Europese richtlijnen - de oude en de verbeterde versie - is om bedrijven beter te beschermen, risico's beter te beheren en incidenten te voorkomen of toch minstens de gevolgen ervan zoveel mogelijk te beperken.

NIS2 maakt deel uit van een groeiende golf van EU-eisen voor cybersecurity, van de eIDAS-verordening uit 2014 tot de GPSR-richtlijn uit 2023. Binnen die gestaag uitdijende EU-wetgeving onderscheidt NIS2 zich door zijn **verregaande reikwijdte** en **diepgaande impact op de gehele organisatie**, en dus niet slechts op een onderdeel ervan of één enkele dienst of technologie, of één enkel product.

Om te beginnen bestrijkt NIS2 liefst **18 sectoren** – 11 meer dan de eerste versie – en is de richtlijn van toepassing op **meer dan 180.000 bedrijven binnen de Europese Unie.** Volgens een eerste schatting van het Centrum voor Cybersecurity België (CCB) zouden er zo'n 2.400 Belgische bedrijven onder de nieuwe Europese richtlijn vallen. Inetum gaat uit van een schatting van zo'n 3.000 bedrijven. Maar wat ook het uiteindelijke cijfer wordt, NIS2 geldt sowieso als **de meest uitgebreide EU-wetgeving op het gebied van cybersecurity tot nu toe.**

> NIS2 is hoe dan ook, of u er nu onder valt of niet, een belangrijke wet.
>
> **Levi Nietvelt,**
> *Beltug*

De supplychain zet (extra) druk

Het toepassingsgebied van NIS2 reikt niet alleen verder dan de originele richtlijn, de impact op de bedrijven die eronder vallen is ook aanzienlijk groter. Zo zijn de **eisen** die de EU aan die bedrijven stelt - ook op het vlak van **rapportering**, bijvoorbeeld - merkelijk zwaarder en strenger dan voorheen.

Hetzelfde geldt voor de **sancties** die de bedrijven in kwestie kunnen oplopen als ze niet aan de gestelde eisen weten te voldoen. Naast **administratieve geldboetes**, het aanwijzen van een toezichthouder en het opschorten van certificeringen of autorisaties, om maar enkele sancties te noemen, kan het niet naleven van de richtlijn voortaan ook **juridische gevolgen voor het senior management** met zich meebrengen. Zo kan zelfs de CEO van het bedrijf nu tijdelijk het verbod opgelegd krijgen om een leidinggevende functie uit te oefenen.

De nieuwe NIS2-richtlijn legt ook heel sterk het accent op het garanderen van de **bedrijfszekerheid (business continuity)**. Die beveiligingseis strekt zich bovendien uit tot de gehele supplychain. Als gevolg van die verscherpte aandacht voor het **beveiligen van de supplychain** is het in veel gevallen aangewezen om toch aan de NIS-richtlijn te voldoen, ook al is die niet direct van toepassing op uw bedrijf. Door eenzelfde compliance op te leggen doorheen hun leveranciersketen kunnen bedrijven immers datalekken vermijden of hackers bannen die anders misschien via hun toeleveranciers alsnog cyberproblemen zouden veroorzaken.

> Scherp gesteld: de speeltijd is voorbij. Europa wil dat alle bedrijven een minimumniveau voor cybersecurity behalen. De NIS2-richtlijn is een hefboom om versneld die veilige ondergrens te bereiken.
>
> **Koen Tamsyn,**
> *Solution Manager*
> *Cybersecurity, Inetum*

Ook de tijd dringt!

Het voorstel voor de nieuwe Europese cybersecurityrichtlijn NIS2 werd in december 2020 door de Europese Commissie ingediend. Na een snel onderhandelingsproces werd de definitieve tekst twee jaar later door de Raad en het Europees Parlement aangenomen, op 27 december 2022 gepubliceerd, om in **januari 2023 officieel in werking** te treden.

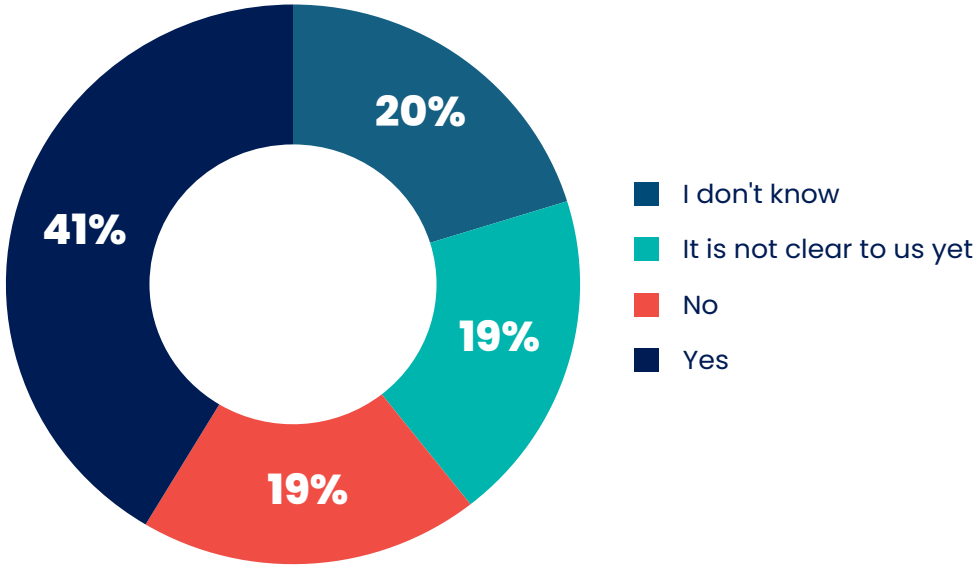
België heeft vervolgens, net als alle andere lidstaten van de EU, 21 maanden de tijd, tot oktober 2024, om de NIS2-richtlijn om te zetten in nationale wetgeving. De federale ministerraad zorgde al op **10 november 2023** voor die **omzetting in Belgisch recht**. De verwachting is dat de wet in april goedgekeurd wordt in het parlement.

Naar verwachting zal NIS2 vanaf oktober 2024 ook in België de bestaande NIS-richtlijn vervangen. Vanaf dat moment moeten alle betrokken bedrijven en organisaties in regel zijn met deze nieuwe regelgeving. Indien er zich een cyberincident zou voordoen, kan u als bedrijf immers hiervoor verantwoordelijk worden gehouden en kunnen er sancties worden opgelegd.

> Oktober 2024 komt er heel snel aan. Ik moedig iedereen dan ook sterk aan om niet te wachten tot de nieuwe wet van toepassing is, en zo snel als mogelijk te starten met het traject om aan alle verplichtingen te voldoen.
>
> **Koen Tamsyn,**
> *Solution Manager*
> *Cybersecurity, Inetum*

To comply, or not to comply, that is the question

Does your organisation need to comply with the NIS2 directive?
All marks (n=303)



Is de NIS2-richtlijn van toepassing op uw organisatie? Op die vraag uit het jaarlijkse prioriteitenonderzoek van Beltug moesten in 2023 nog vier op de tien Belgische bedrijven (39%) het antwoord schuldig blijven. De helft van die bedrijven had er gewoonweg geen idee van, terwijl het voor de andere helft nog onvoldoende duidelijk was of ze al dan niet onder de richtlijn vielen.

De volgende twee criteria helpen dat voor u bepalen:

Criterium 1: sector

De NIS2-richtlijn is van toepassing op alle sectoren die al onder de eerste NIS-richtlijn vielen, maar ook op een aantal nieuwe sectoren, wat het totaal op **18 sectoren** brengt. Het aantal organisaties dat onder de richtlijn valt, neemt daardoor toe.

De NIS2-richtlijn maakt daarbij een onderscheid tussen **kritieke** en **zeer kritieke** sectoren:

Kritieke Sectoren

- Afvalstoffenbeheer
- Chemische stoffen
- Digitale aanbieders
- Levensmiddelen
- Onderzoek
- Post- en koerierdiensten
- Maakbedrijven (manufacturing)

Zeer Kritieke Sectoren

- Afvalwater
- Bankwezen
- Beheerders van ICT-diensten
- Digitale infrastructuur
- Drinkwater
- Energie
- Gezondheidszorg
- Infrastructuur financiële markt
- Overheidsdiensten
- Ruimtevaart
- Transport

Criterium 2: omvang en kriticiteit

Een belangrijk verschil met de eerste NIS-richtlijn is dat organisaties automatisch onder de NIS2-richtlijn vallen als zij actief zijn in een van de bovenstaande sectoren en gekenmerkt kunnen worden als '**essentiële**' of '**belangrijke**' **entiteit**. Die kwalificatie is afhankelijk van factoren zoals de **sector**, maar ook de **omvang**, uitgedrukt in omzet en aantal werknemers, en de **kriticiteit** van de organisatie.

In **kritieke sectoren** is bijvoorbeeld geen enkel type van bedrijf essentieel, maar zijn ze allemaal **belangrijk**. Met uitzondering van bedrijven die minder dan 50 voltijdse medewerkers in dienst hebben én minder dan 10 miljoen euro omzet draaien: op hen is NIS2 simpelweg niet van toepassing.

Dat laatste geldt trouwens ook voor bedrijven in **zeer kritieke sectoren**. Daar vind je dan weer wel een aantal essentiële bedrijven terug, naast belangrijke. Essentieel zijn zo goed als alle bedrijven die meer dan 250 voltijdse medewerkers tewerkstellen, onafhankelijk van de omzet die ze draaien, alsook een aantal bedrijven die meer dan 50 miljoen euro omzet realiseren, onafhankelijk van het aantal medewerkers dat ze in dienst hebben. Voor die essentiële bedrijven is de **richtlijn strenger** omdat over het algemeen wordt aangenomen dat de uitval van hun diensten een veel meer **ontwrichtende impact** heeft op de economie en samenleving dan de uitval bij belangrijke bedrijven.

> Stel je minder dan 50 mensen tewerk, dan val je niet onder NIS2. Maar wees voorzichtig. Want lever je kritische diensten of producten aan bedrijven die wel onder NIS2 vallen, dan zal je hun moeten aantonen dat je veilig opereert, desnoods via een officiële audit. Zij zijn immers verantwoordelijk voor hun supplychain-risico.
>
> **Arnaud Martin,**
> *Agoria*

NIS2-compliant worden: wat betekent dat voor u?

Valt uw bedrijf op basis van bovenstaande criteria onder de NIS2-richtlijn? Dan worden er grosso modo twee belangrijke eisen aan u gesteld.

Ten eerste moet u een aantal **maatregelen nemen om uw risico's op het gebied van cybersecurity voldoende te kunnen beheersen en beperken.** Dat kunnen zowel technische en operationele als organisatorische maatregelen zijn. Belangrijk is vooral dat ze passend en proportioneel zijn. Concreet gaat het om maatregelen in deze tien domeinen:

1. Risicoanalyse en -beheer
2. Beveiligingsbeleid en activabeheer
3. Incidentafhandeling (preventie, detectie en reactie op incidenten)
4. Bedrijfscontinuïteit en crisismanagement
5. Beveiliging van de supplychain (kwetsbaarheden van leveranciers in rekening brengen)
6. Beheer en afhandeling van kwetsbaarheden
7. Regelmatige beoordelingen (assessments)
8. Het gebruik van encryptie waar nodig
9. Basishygiëne en training op het gebied van cybersecurity
10. Het gebruik van multifactorauthenticatie (MFA) of continue authenticatie

Ten tweede moet u ook aan een aantal verplichtingen voldoen voor het **melden van incidenten.** Zo moet u significante incidenten voortaan onverwijld – om precies te zijn: **binnen de 24 uren** – melden aan het Computer Security Incident Response Team (CSIRT) of de relevante bevoegde autoriteit. Na maximaal **drie dagen (72 uren)** moet daarop een uitgebreider voortgangsrapport volgen. Ten laatste **een maand** na melding moet u het finale rapport over het incident kunnen voorleggen, inclusief de genomen maatregelen die al dan niet nog zijn doorlopen.

> Je moet weten: welk risico loop ik vandaag? En hoe kan ik dat risico terugbrengen tot op een acceptabel niveau?
>
> **Koen Tamsyn,**
> *Solution Manager Cybersecurity, Inetum*

Hulp nodig? Inetum springt graag bij!

Heeft u zelf niet de nodige mensen of middelen in huis om de naleving van de NIS2-richtlijn vlot te verzekeren? Of ziet u steeds meer op tegen de bijkomende last die zo'n ingrijpende operatie met zich meebrengt?

Bij Inetum begrijpen we niet alleen het belang en de noodzaak om te voldoen aan regelgevende kaders zoals NIS2, wij beschikken ook over de **experts** en de **oplossingen** om u succesvol bij te staan op uw traject naar compliance - met raad én daad.

Ad-hocadvies / Consultancy

U kan beroep doen op ons team van cybersecurityspecialisten om uw huidige beveiligingspositie te analyseren en te beoordelen. Op basis van dat voorbereidende **assessment** kunnen zij vervolgens ook een aangepast **beveiligingsplan** ontwikkelen dat aan uw specifieke behoeften tegemoetkomt.

Om u te helpen voldoen aan de minimale maatregelen die NIS2 vereist, bieden wij ten slotte ook een brede waaier aan hulpmiddelen en begeleiding, zoals **risicobeoordelingen, beveiligingsprocedures** en **incidentresponsplannen**.

> Assessments om te beoordelen hoe ver een bedrijf staat op het vlak van cybersecurity doen wij al langer dan vandaag. Recent hebben wij die dienstverlening nog een update gegeven en helemaal aangepast aan de NIS2-maatregelen.
>
> **Koen Tamsyn,**
> *Solution Manager*
> *Cybersecurity, Inetum*

Cybersecurity Roadmap

Via onze Cybersecurity Roadmap brengen we in drie stappen uw **maturiteit** op het vlak van cybersecurity in kaart en analyseren eventuele **zwaktes** in functie van uw NIS2-implementatie. Op basis van die momentopname formuleren wij uiteindelijk ook concrete **optimalisatievoorstellen**.

Onze cybersecurity roadmap bestaat uit een technologieluik in de vorm van een **datascan** en een niet-technisch luik waarbij u een **vragenlijst** beantwoordt in het kader van een **workshop**.

Tijdens het assessment doorlopen we samen deze **drie stappen:**

Stap 1: voorbereiding van uw assessment

We organiseren een kick-offgesprek met een cybersecurityspecialist om elkaar beter te leren kennen, de **doelstellingen** van uw assessment te bespreken en de **systeemvereisten** te delen. Dat stelt ons in staat om uw IT-omgeving optimaal voor te bereiden op het eigenlijke assessment.

Stap 2: uw IT-middelen: gegevensverzameling en -analyse

We installeren een tool in uw IT-omgeving die verbinding maakt met allerlei **platformen**, zowel lokaal (Active Directory, SharePoint, email DNS, endpoints en servers) als in de **cloud** (Azure, Microsoft 365, …). Daarmee voert een van onze cybersecurityspecialisten de nodige scans en tests uit om alle relevante data te verzamelen. Aan de hand van een vaste **vragenlijst** nemen we ook een **interview** af van uw CIO of CISO. Daarin bespreken we de cybersecuritypositie van uw organisatie.

Stap 3: presentatie van uw eindrapport

Tijdens een presentatie delen we onze bevindingen, conclusies en aanbevelingen met u. Daarna bezorgen we u die **managementpresentatie**, samen met het uitgebreide **eindrapport**.

CISO as a service

Cybersecurity is echter geen statisch gegeven, maar een **cyclisch proces**. Noem het gerust een eeuwig 'work-in-progress' om enerzijds uw cybersecuritydoelen te blijven afstemmen op uw algemene bedrijfsdoelstellingen en strategieën voor risicobeheer, anderzijds compliant te blijven met regelgevingen. NIS2 draait niet alleen **om technologische oplossingen**, maar ook rond **policies & procedures**.

Er is een hele lijst van 'must-haves' als u wilt slagen voor een NIS2-audit. Denken we maar aan een policy voor information security, access control, incident response, cryptography, vendor management, data classification and handling, enz…

Is een voltijdse CISO voor u nog te hoog gegrepen? Dan stellen wij graag onze CISO as a Service aan u voor: een security-expert die deeltijds de rol van CISO bij u komt opnemen.

Samen maken wij er werk van

Valt uw bedrijf onder de NIS2-richtlijn of bent u een belangrijke leverancier voor een bedrijf dat valt onder NIS2? Dan raden wij u aan om nu alvast werk te maken van een cybersecurity assessment en samen met ons ook een cybersecurity roadmap op te stellen. Zo heeft u voldoende tijd om de noodzakelijke maatregelen te nemen om veilig te kunnen (blijven) opereren, in overeenstemming met die nieuwe NIS-richtlijn. Bovendien laat die doordachte, gefaseerde aanpak u toe om niet alleen het werk maar ook de kosten te spreiden.

NEEM CONTACT OP

Inetum
A. Vaucampslaan 42
1654 Huizingen, België
+32 2 801 55 55
www.inetum-realdolmen.world
info@inetum-realdolmen.world

inetum