


# Maturiteitsgids voor digitale dienstverleners

05 september 2023, 16:47

Tatiana Galibus

## Hoe u goed voorbereiden op de NIS2-richtlijn

Het is geen geheim dat er met de nieuwe NIS2-richtlijn een serieuze verschuiving wordt verwacht voor digitale dienstverleners. De opkomende regelgeving zal veel digitale providers en datacenters ertoe aanzetten zich als essentiële of belangrijke entiteiten op te stellen. De broeksriem wordt voor bijna iedereen aangespannen: zodra een dienstverlener een belangrijke klant heeft die onder de NIS-regelgeving valt, komt hij automatisch in een vertrouwensrelatie terecht, en dient hij de beveiligingsvragen te beantwoorden en aansluitend een audit uit te voeren. Softwarebedrijven, zelfs start-ups en scale-ups, moeten de regelgeving ter zake nauwgezetter volgen en worden vaak hiertoe met aandrang aangezet door de klanten zelf.

### Welke normen gelden in België?

De NIS2-richtlijn legt geen stapsgewijze richtlijnen op voor bedrijven. Lidstaten passen de algemene regels aan hun eigen situatie aan om de naleving te garanderen. In België gebeurt dit onder toezicht van het Center for Cybersecurity Belgium binnen het kader van het Cyberfundamentals framework. Cyberfundamentals is vrij generiek en hoewel aangepast voor kmo’s, is het niet specifiek voor softwarebedrijven, ontwikkelaars, testers, datacenters, digitale

dienstverleners, enz.

## Welke zijn de cyberbeveiligingsnormen voor softwarebouwers?

Het goede nieuws is dat er een goed gedefinieerd, vertrouwd kader van richtlijnen en tools bestaat voor de beveiliging van digitale diensten. Ondersteund door OWASP, zet deze non-profitorganisatie zich in voor het verbeteren van softwarebeveiliging. OWASP biedt en ontwikkelt verschillende belangrijke, door digitale bedrijven na te leven normen.

Waarom softwarebouwers deze normen onder de loep zouden moeten nemen? Ze zijn bruikbaar, begrijpelijk, pragmatisch en wereldwijd toegepast door beveiligingsexperts van softwarebedrijven.

- OWASP ASVS
- OWASP DSOMM
- OWASP SAMM

## OWASP ASVS

De OWASP Application Security Verification Standard (ASVS) biedt een basislijst met vereisten voor veilige ontwikkeling. We raden deze norm aan voor ontwikkelaars en testers. ASVS stelt drie maturiteitsniveaus voor:

| NIVEAU | VOOR WIE |
|---|---|
| ASVS niveau 1 | Een basisniveau van betrouwbaarheid dat kan worden beoordeeld met minder interac het applicatieteam. |
| ASVS niveau 2 | Een niveau van betrouwbaarheid voor de meeste applicaties die gevoelige gegevens b |
| ASVS niveau 3 | Voorbehouden voor de meest kritische applicaties, waarvoor een significante integratie het applicatieteam nodig is. |

## OWASP DSOMM

De OWASP DevSecOps Maturity Model biedt mogelijkheden voor het verbeteren en prioriteren van de DevOps-strategieën. Het biedt vereisten en implementatieniveaus voor de automatisering van pipelines, softwareontwikkeling en het verbeteren van de infrastructuur. We raden deze norm aan voor automatiseringsoperatoren, testers, solution managers en projectleiders. DSOMM stelt vijf maturiteitsniveaus voor (we geven een overzicht van de eerste drie):

| NIVEAU | VOOR WIE | CONTROLES |
|---|---|---|
| DSOMM niveau 1 | Basiskennis van beveiligingspraktijken | 23 controles |

| | |
|---|---|
| DSOMM niveau 2 Invoering van basisbeveiligingspraktijken | 47 controles |
| DSOMM niveau 3 Hoge mate van toepassing van beveiligingspraktijken | 45 controles |

## OWASP SAMM

De Software Assurance Maturity Model (SAMM) is een open framework om organisaties te helpen bij het formuleren en implementeren van een strategie voor softwarebeveiliging die is afgestemd op de specifieke risico's van de organisatie. Het model helpt om bestaande softwarebeveiligingspraktijken van een organisatie te evalueren en een gebalanceerd programma voor de betrouwbaarheid van softwarebeveiliging op te stellen.

We raden deze norm aan voor CEO's, projectleiders en projecteigenaars. Het model is gebaseerd op de kernfuncties van softwareontwikkeling met beveiligingspraktijken die aan elke functie zijn gekoppeld (zie onderstaand schema). De bouwstenen van het model zijn de drie


nieerd:

## Hoe kan Sirris helpen?

Op **18 oktober 2023** organiseert Sirris een **expertsessie voor kennisuitwisseling** gericht op de NIS2-richtlijn en andere opkomende cyberbeveiligingsbehoeften voor digitale diensten. De sessie is volledig gratis. In deze online meeting kunt u de mening van experts over de nieuwe regelgeving en cyberbeveiligingsuitdagingen horen en van gedachten wisselen met de alumni van onze masterclass over hun reis naar cyberbeveiligingsmaturiteit.

U kunt zich hier inschrijven.

Deze sessie zal ook de kick-off zijn van onze **Cybersecurity bootcamp voor SaaS en digitale diensten**, gesubsidieerd door VLAIO voor Vlaamse bedrijven. Het bootcamp is ontworpen als een leerreis, met grondige theoretische sessies en praktijksessies op maat. We werken samen met cyberbeveiligingsaanbieders in heel Vlaanderen om de beste leer- en netwerkervaring te bieden, evenals individuele micro-coaching-sessies voor uw individuele noden.

Meer weten over het bootcamp en hoe in te schrijven? Surf naar onze agenda!

# Auteurs



Tatiana Galibus