NIS2 komt eraan

In Europa is een NIS (Network and Information Systems) directive opgesteld om bij te dragen aan een hoog gemeenschappelijk beveiligingsniveau van netwerk- en informatiesystemen in de hele EU. Al in 2016 is de NIS1-richtlijn gepubliceerd. Deze was met name bedoeld voor grote bedrijven en instellingen die essentiële functies voor de samenleving vervullen. Denk aan Stroom, Netwerk en Watervoorziening leveranciers. Zij zijn al enkele jaren verplicht om informatiebeveiliging maatregelen te nemen om de cyberweerbaarheid te verhogen.

NIS2

In mei 2022 is de Europese Commissie akkoord gegaan met een nieuwe versie, de NIS2. In deze versie is de scope verruimd waarvoor deze directive van toepassing is. Denk daarbij aan de maakindustrie voor kritische producten, de ICT dienstenleveranciers (MSP), maar ook aan alle zorgverleners (denk aan Ziekenhuizen en alle andere zorgverleners)

De Europese commissie schrijft hierover;

“Om het hoofd te bieden aan de toenemende cyberdreigingen in Europa, is de NIS 2-richtlijn nu van toepassing op middelgrote en grote entiteiten uit meer sectoren die van cruciaal belang zijn voor de economie en de samenleving, waaronder aanbieders van openbare elektronische-communicatiediensten, digitale diensten, afvalwater- en afvalbeheer, de vervaardiging van kritieke producten, post- en koeriersdiensten en overheidsdiensten, zowel op centraal als regionaal niveau.

Zij bestrijkt ook meer in het algemeen de gezondheidszorg, bijvoorbeeld fabrikanten van medische hulpmiddelen, gezien de toenemende veiligheidsdreigingen die zich tijdens de coronapandemie hebben voorgedaan. De uitbreiding van het toepassingsgebied van de nieuwe regels, door meer entiteiten en sectoren te verplichten maatregelen te nemen om cyberbeveiligingsrisico’s te beheersen, helpt het cyberbeveiligingsniveau in Europa op middellange en lange termijn te verhogen.

bron Europese Commissie

Wetgeving

De NIS2 is een Europese richtlijn en moet nu worden omzet naar lokale wetgeving. De Nederlandse overheid heeft 21 maanden de tijd, om deze richtlijn om te zetten naar Nederlandse wetgeving. Dus voor Maart 2024 zal er ook Nederlandse wetgeving komen.

Wat betekend dit dan?

Het gevolg hiervan is dat veel meer organisaties verplicht zijn om maatregelen te nemen t.b.v. informatiebeveiliging. Alle zorginstellingen kunnen hiermee verplicht worden gesteld om aan de NEN7510 te gaan voldoen. Maar ook kleinere ICT-dienstverlener (MSP) die voor grotere organisaties het netwerk beheren worden verplicht om aantoonbaar aan de ISO27001 te voldoen. Maar denk ook aan de maak-industrie, zij moeten ook verplicht voldoen aan de ISO27001 norm. Werk aan de winkel dus. Of jouw organisatie kritieke-producten maakt, wordt later dus meer helder. Maar enige ‘jan-boeren-verstand’ kan je ook al helpen om nu al je eigen conclusie te trekken of je tot deze categorie gaat behoren.

Tijd om actie te ondernemen

Ons advies is om niet te wachten totdat je op je vingers wordt getikt door inspectie, denk aan IGJ of een andere inspecteur. Ga nu aan de slag en neem actie. Hoe, dat is per organisatie afhankelijk. Wat heb je al wel en wat niet.

Om te weten waar je staat, kunnen we een Nul-meting (pre-audit) voor u uitvoeren. 12secure-u geeft advies HOE u moet gaan voldoen in samenwerking met uw organisatie. Ook kunnen we u, geheel onafhankelijk een helder beeld scheppen waar u nu staat mbt het voldoen aan de ISO27001 of NEN7510.