NIS2

Voorbereid zijn op de Nieuwe Europese Cybersecurity Wetgeving

SECURITY IS AL LANG NIET MEER ALLEEN EEN IT-FEESTJE! DE IMPACT VAN EEN CYBERAANVAL IS VOOR DE MEESTE ORGANISATIES ZEER GROOT (GEMIDDELD BEDRAGEN DE KOSTEN NA EEN HACK 300.000 EURO) EN DE KANS DAT JE ALS ORGANISATIE TE MAKEN KRIJGT MET EEN CYBERAANVAL IS GROOT.... VEEL GROTER DAN DE MEESTE MENSEN DENKEN, NAMELIJK VEERTIG KEER GROTER DAN BIJVOORBEELD DE KANS OP EEN BRAND. DE EU ERKENT DE CYBERSECURITY-UITDAGINGEN WAAR WE VOOR STAAN EN LEGT MET DE NIS2 STRENGERE REGELS OP AAN STEEDS MEER ORGANISATIES.

Door Bouke van Kleef

NIS2 vanaf oktober 2024
Veel organisaties worden door wet- en regelgeving (AVG, BIO) of door hun eigen ambities (bijvoorbeeld met een ISO 27001-certificering) min of meer gedwongen om hun cybersecurity op orde te hebben. De nieuwste prikkel hiervoor is de NIS2. De NIS2 (NIS: Netwerk en Informatie Systemen) is een nieuwe Europese wetgeving/richtlijn die vanaf oktober 2024 van kracht wordt voor kritische infrastructuur en essentiële bedrijven. Het doel van de NIS2 is om de cyberbeveiliging van essentiële en belangrijke sectoren te verbeteren en te harmoniseren. Deze richtlijn vervangt de bestaande NIS-richtlijn uit 2016 en stelt strengere eisen aan de beveiliging en melding van cyberincidenten. NIS2 moet voor oktober 2024 in nationale wetgeving worden omgezet. Ik verwacht dat de NIS2, net als de Algemene Verordening Gegevensbescherming (AVG), op veel organisaties impact gaat hebben. Ik merk dat veel organisaties er nog niet klaar voor zijn.

Belangrijk om te weten: ook als jouw organisatie géén onderdeel is van de essentiële en belangrijke sectoren, maar wél levert aan deze sectoren, heb je verplichtingen ten aanzien van de NIS2 richtlijnen. De security moet namelijk binnen de gehele keten worden gewaarborgd; van essentiële organisaties en sectoren tot hun toeleveranciers én hun onderaannemers. (Zie ook het artikel op de site van 'Samen Digitaal Veilig' door MKB Nederland over toeleveranciers die onder de NIS2 vallen).

Enkele belangrijke verschillen met voorganger NIS:

- Meer organisaties moeten voldoen: meer organisaties vallen onder de NIS2. Naast kritische infrastructuur zoals water, energie en gas, nu ook bijvoorbeeld IT-dienstverleners, clouddiensten, zorgaanbieders en gemeenten.
- Leveranciers moeten ook voldoen: organisaties die leveren aan kritische infrastructuur krijgen ook te maken met NIS2, omdat de organisaties die vallen onder NIS2 aanvullende eisen moeten opleggen aan hun ketenpartners.
- Bestuurdersaansprakelijkheid: bestuurders die verwijtbaar niet voldoen aan NIS2 zijn hoofdelijk aansprakelijk volgens de NIS2.
- Datalekken moeten binnen 24 uur worden gemeld, ook als ze bijvoorbeeld door een leverancier zijn veroorzaakt. Dit is vergelijkbaar met de vereisten van de AVG, maar met een termijn van 24 uur in plaats van 72 uur.

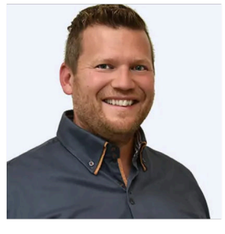
Als ambtelijk secretaris is het belangrijk om op de hoogte te zijn van deze nieuwe wetgeving en de impact die het kan hebben op de organisatie. De NIS2 stelt meer eisen aan de beveiliging en melding van cyberincidenten en moet uiterlijk voor oktober 2024 worden omgezet in nationale wetgeving.

Als ambtelijk secretaris kun je een belangrijke rol spelen bij het voorbereiden van jouw organisatie op de komst van de NIS2. Dit kan door het informeren van het management en het personeel over de nieuwe wetgeving en de eisen die het stelt aan de beveiliging en melding van cyberincidenten. Ook kun je helpen bij het opstellen van een plan van aanpak om te voldoen aan de eisen van de NIS2.

De ambtelijk secretaris kan de OR stimuleren om de organisatie voor te bereiden op de NIS2:

- Het gesprek aangaan met directie/bestuur om te bepalen welke impact de NIS2 heeft op de organisatie. Valt de organisatie onder essentiële of kritische infrastructuur of alleen als toeleverancier?
- Voer gesprekken met de (interne) specialisten zoals de huisjurist, IT en/of security officer.
- Ga na of de organisatie al voldoet aan bijvoorbeeld de ISO27001 of de BIO. Veel van de eisen vanuit de NIS2 worden afgedekt wanneer de organisatie al voldoet aan de ISO27001.
- Vraag na of er al een nulmeting, een scan of een audit heeft plaatsgevonden. Zo kun je de kloof identificeren tussen de huidige beveiligingsmaatregelen en de eisen van de NIS2.
- Zorg dat personeel 'digitaal vitaal' is. Vraag na hoe het staat met het trainen van de collega's ten aanzien van digitale vaardigheid, privacy en security awareness. Kennis rondom security is namelijk niet een eenmalige interventie. Er is doorlopend aandacht nodig voor security.
- Tot slot kan de ambtelijk secretaris een rol spelen bij het monitoren en rapporteren van de voortgang en de resultaten van de implementatie.

De toekomst is digitaal, AVK Training & Coaching helpt je organisatie **Digitaal Vitaal** (https://avk.nl/digitaal-vitaal/) te zijn, en dankzij deze nieuwe EU-wetgeving, worden we min of meer gedwongen de basis security beter op orde te hebben.



BOUKE VAN KLEEF
AVK Training & Coaching

AVK
(https://www.avk.nl/)

Telefoon: 085 208 33 88
E-mail: info@avk.nl