Hands on ICT
Alles over NIS2

Maak jouw organisatie NIS2 proof

www.handsonict.nl

Waar staat NIS2 voor?

NIS2 staat voor Network and Information Systems Security Directive en heeft als doel de digitale beveiliging te verbeteren en de impact van cyberincidenten te verminderen. Deze richtlijn beïnvloedt organisaties in verschillende sectoren en is bedoeld om de digitale infrastructuur in Europa te beschermen. NIS2 is op 27 december 2022 gepubliceerd. Echter hebben alle Europese landen tot 17 oktober 2024 om de richtlijn in nationale wet- en regelgeving te implementeren.

De impact

Deze regelgeving kan een grote impact hebben op jouw organisatie. We begrijpen dat het voor de meeste organisaties een grote uitdaging is om zich voor te bereiden op NIS2. We staan klaar om je hierbij te ondersteunen. Met onze YourSecurity service bieden we een uitgebreid assortiment aan diensten en producten die ervoor zorgen dat je altijd en overal veilig kunt werken, terwijl je waardevolle bedrijfsdata goed beveiligd is. Op deze manier kun je je alvast voorbereiden op de aanstaande regelgeving en tegelijkertijd je organisatie effectief beschermen tegen cybercriminaliteit.

Voor wie geldt NIS2?

De NIS-richtlijn omvatte oorspronkelijk twee sectoren: kritieke infrastructuren en Digital Service Providers (DSP's). De NIS2-richtlijn breidt deze sectoren niet alleen uit, maar stelt ook strengere richtlijnen vast voor het definiëren van aanbieders die van cruciaal belang zijn voor de maatschappij. Hieronder vallen sectoren zoals gezondheidszorg, transport, energieleveranciers, overheidsdiensten, voedselvoorziening, waterbeheerbedrijven en digitale dienstverleners. Bovendien wordt de NIS2-richtlijn uitgebreid naar wat wordt aangeduid als 'belangrijke sectoren'.

Met de nieuwe NIS2-regelgeving is de definitie van het begrip 'vitaal belang' verruimd. Zelfs als

Is jouw organisatie al NIS2 proof?

Weet jij al of jouw organisatie onder de NIS2-richtlijn valt? Kom niet voor verrassingen te staan en doe hier de NIS2 snelscan.

Download hieronder onze snelscan PDF:

Snelscan

Wat zijn jouw verplichtingen?

Alle organisaties die onder de NIS2-richtlijn vallen, moeten aan bepaalde eisen voldoen. Hieronder lees je alle verplichtingen.

Zorgplicht

Alle organisaties die onder de NIS2-richtlijn vallen, moeten voldoen aan hun zorgplicht. Dit houdt in dat ze bepaalde maatregelen moeten nemen. Denk hierbij aan het opzetten van plannen voor als er een groot cyberincident plaatsvindt en het gebruik van versleuteling en beveiliging van informatie. De richtlijnen voor de zorgplicht bevatten verschillende soorten maatregelen die organisaties moeten nemen om ervoor te zorgen dat hun informatiesystemen veilig en betrouwbaar zijn.

De richtlijnen voor de zorgplicht zijn: **Risico analyse, beveiligingsbeleid, incidentenbeheer en training & bewustwording.**

Meldplicht

Er geldt een meldingsverplichting voor alle organisaties die onder de NIS2-wetgeving vallen. Dat betekent dat zij binnen 24 uur na ontdekking van een incident moeten melden. Binnen een maand moet deze melding worden aangevuld met een meer gedetailleerd rapport. De meldplicht omvat specifieke aspecten met betrekking tot het melden van incidenten.gebruikers binnen je organisatie wordt geïnstalleerd in Outlook kunnen je medewerkers phishingmails direct rapporteren.

maand moet deze melding worden aangevuld met een meer gedetailleerd rapport. De meldplicht omvat specifieke aspecten met betrekking tot het melden van incidenten.

De meldplicht omvat deze zaken rondom incidentmeldingen: **Daadwerkelijk schadelijk effect, operationele verstoring of financiële verliezen en bij materiële of immateriële schade.**

Toezicht en naleving

Een aanzienlijk onderscheid tussen NIS2 en NIS ligt in de uitbreiding van het toezicht. Voorheen hadden lidstaten meer vrijheid wat betreft de mate van toezicht. NIS2 streeft echter naar een strenger gereguleerd toezicht, wat inhoudt dat er specifieke richtlijnen zullen worden vastgesteld voor toezichthoudende instanties.

Een boete voor het niet naleven (non-compliance) wordt voorgesteld in NIS2, wat lijkt op de aanpak van de Algemene Verordening Gegevensbescherming (AVG), waarbij boetes worden opgelegd voor het niet voldoen aan de voorschriften. Dit streven beoogt een meer consistente handhaving van de NIS-regels tussen verschillende lidstaten.

Wat betekent dit voor mijn organisatie?

Het is van essentieel belang dat elke organisatie maatregelen neemt om zich te verweren tegen cyberaanvallen en zo daarmee te voldoen aan de NIS2 wetgeving.

1. Risicoanalyse
Voer een risicoanalyse uit om de meest kritieke data en systemen te identificeren en het bijbehorende risico op een hack te beoordelen.

Hiermee identificeer je potentiële risico's op data en systemen. Daarnaast is het belangrijk om een Business Impact Analysis (BIA) uit te voeren om de impact van deze risico's op de bedrijfsvoering te begrijpen.

2. Maatregelen bedrijfscontinuïteit
Ontwikkel een bedrijfscontinuïteitsplan

Op basis van de risicoanalyse en BIA moet een bedrijfscontinuïteitsplan worden ontwikkeld. Dit plan moet specifieke maatregelen bevatten om de geïdentificeerde risico's aan te pakken en de bedrijfscontinuïteit te waarborgen.

3. Beoordeling veiligheid in keten
Beoordeel de veiligheid in de keten om potentiële risico's van externe leveranciers en dienstverleners te identificeren volgens de richtlijnen van NIS2.

Als het gaat om het beoordelen van de veiligheid in de keten en het identificeren van potentiële risico's van externe leveranciers en dienstverleners volgens de richtlijnen van NIS2, is het van belang om passende maatregelen voor bedrijfscontinuïteit te nemen. Bedrijfscontinuïteit richt zich op het waarborgen dat een organisatie blijft functioneren, zelfs in het geval van onvoorziene gebeurtenissen of verstoringen

4. Beveiliging van netwerk- en informatiesystemen
Neem maatregelen voor de beveiliging van netwerk- en informatiesystemen, met specifieke aandacht voor de inrichting ervan en het omgaan met kwetsbaarheden.

Ga aan de slag met een uitgebreide aanpak voor de beveiliging van netwerk- en informatiesystemen, waarbij systemen goed zijn ingericht en er een doeltreffend beleid is voor het identificeren en omgaan met kwetsbaarheden.

5. Cyberveiligheidsbeleid
Zorg er voor dat het personeel binnen uw organisatie op de hoogte is van het cyberveiligheidsbeleid en wordt nageleefd

Om het cyberveiligheidsbeleid te waarborgen is het raadzaam om een trainingsprogramma te implementeren, waardoor alle medewerkers goed op de hoogte zijn van het beleid. Zorg er ook voor dat er consistent gehandeld wordt in overeenstemming met dit beleid. Zorg naast beleidstrainingen ook voor awareness trainingen om algehele bewustwording te krijgen voor je medewerkers.

6. Effectiviteit cybersecurity maatregelen
Beoordeel grondig de staat en effectiviteit van het beleid en procedures om de doeltreffendheid van de cybersecurity maatregelen te toetsen.

Met een grondige beoordeling van het beleid en procedures creëer je een duidelijk inzicht in de effectiviteit van de maatregelen, waardoor je passende verbeteringen kunt doorvoeren.

7. Cryptografie en encryptie implementatie
Voer een duidelijk beleid waarin gedetailleerd procedures zijn vastgesteld voor het gebruik van cryptografie en encryptie.

Met een duidelijk en gedetailleerd beleid kun je zorgvuldig controleren of kritieke systemen uitsluitend toegankelijk zijn via goed beveiligde en correct versleutelde verbindingen.

8. Fysieke beveiliging
Neem maatregelen binnen je organisatie voor fysieke beveiliging, inclusief beleid met betrekking tot personeel, toegangscontrole en activabeheer.

Met de implementatie van een uitgebreid beleid zorg je ervoor dat alle aspecten van de fysieke veiligheid van het personeel worden gewaarborgd.

9. Multifactor authenticatie
Pas multifactor authenticatie (2FA) toe binnen je organisatie.

Zorg dat je Multifactor authenticatie toepast op alle relevante accounts, inclusief die vanaf het internet toegankelijk zijn en beheerrechten hebben van essentiële systemen. Zo kun je je organisatie optimaal beveiligen tegen cybercriminelen.

Financiële gevolgen en boetes

NIS2 brengt enkele financiële gevolgen met zich mee voor jouw organisatie. Daarnaast kun je forse boetes krijgen als je onder de NIS2-richtlijn valt maar je je niet houdt aan deze regelgeving.

Boetes: wanneer je onder de NIS2-richtlijn valt, maar je je niet houdt aan de regelgeving, kun je een forse boete ontvangen. De maximale hoogte van de boete bedraagt 10 miljoen euro of 2% van de totale wereldwijde omzet.

Financiële gevolgen: NIS2 brengt ook andere financiële gevolgen met zich mee. Organisaties die nu nog niet onder de richtlijn vallen moeten rekening houden met het verhogen van hun ICT-budget met 22%. Organisaties die al te maken hadden met NIS krijgen te maken met een verhoging van 12%.

Schorsing: Bedrijven die zich niet houden aan de NIS2-richtlijn kunnen een schorsing verwachten. In hoeverre schorsingen worden doorgevoerd is momenteel nog niet bekend.

De Security Health Scan

Met onze YourSecurity-service werken we stap voor stap naar een goed beveiligde omgeving toe. We beginnen altijd met een Security Health Scan om de huidige situatie te beoordelen. Vervolgens stellen we een advies op met bijbehorende actiepunten om jouw IT-security te versterken. Op deze manier waarborgen we een veilige omgeving die risico's minimaliseert. Bovendien helpen we je medewerkers alert te zijn op belangrijke signalen en hierop te reageren. Onze YourSecurity-service verloopt volgens de volgende stappen:

Stap #1

Security Health Scan – de 0-meting

We starten met een Security Health Scan van je organisatie. In deze health scan onderzoeken we de belangrijkste facetten rondom IT Security en krijgen we een beeld van de huidige situatie.

Met deze 0-meting hebben we een concrete set aan adviezen en aanbevelingen om je IT Security beter in te richten. Wat is nodig om het vereiste beveiligingsniveau te bereiken? In een helder rapport geven we advies over de noodzakelijke verbeterpunten, welke impact de verbeterpunten hebben op de ICT-omgeving en de organisatie, en welke investeringen nodig zijn om deze punten te realiseren. We komen dit rapport op locatie presenteren en toelichten. De rapportage en het advies zijn inbegrepen in de eenmalige investering voor de Security Health Scan.

Stap #2

Security oplossingen

N.a.v. het advies kunnen we maatwerk oplossingen gaan bieden om je IT Security naar een nog hoger niveau te tillen. Deze maatwerk oplossingen, welke altijd in overleg worden bepaald, vallen buiten de maandelijkse kosten van YourSecurity. Denk hierbij aan het trainen van personeel, MFA-inrichting, bepalen van securitybeleid of inrichting van policies.

Stap #3

Security Management (periodieke scans)

Cybercriminaliteit ontwikkelt op een hoog tempo, zo ook de technieken die ervoor zorgen dat cybercriminelen minder kans maken om binnen te dringen. Met Security Management voeren we een periodieke scan op je omgeving uit zodat je ook in de toekomst geborgd bent van een veilige omgeving. Voor deze actieve monitoring en management op IT security zullen wij diverse monitoringstools inrichten om te zorgen dat bedreigingen van buitenaf direct en proactief worden gesignaleerd en opgelost. Denk hierbij bijvoorbeeld aan endpoint detection, onderhoud en doorvoeren van updates.

Doe hier de Health Scan:

Health Scan

yoursecurity

Meer weten over NIS2?

Check onze website voor meer informatie over NIS2 en waar Hands on ICT jouw organisatie mee kan helpen. Daarnaast kun je vrijblijvend een online call plannen met een van onze accountmangers.

Meer informatie

Contactgegevens
Hands on ICT
Nesland 5a
1382 MZ Weesp
+31(0)88 - 181 1300

info@handsonict.nl
www.handsonict.nl