WAT IS DE IMPACT?

NIS2 Werkboek

Pink Elephant
maakt IT persoonlijk

start

v 1.0

Managementsamenvatting

NIS2 is een richtlijn vanuit de EU om de cybersecurity en cyberweerbaarheid te versterken. De lidstaten vertalen dit naar nationale wetgeving. Hieraan wordt nog gewerkt, maar naar verwachting wordt deze in Nederland in oktober 2024 van kracht. De wet gaat vanaf dat moment automatisch gelden voor organisaties die eronder vallen.

NIS2 wordt van toepassing op essentiële en belangrijke entiteiten in bepaalde sectoren wanneer ze een bepaalde omvang hebben. Daarnaast moeten ook ketenpartners van die enititeiten en andere specifieke organisaties voldoen aan de wet.

NIS2 kent een een zorgplicht, meldplicht en toezicht.

De zorgplicht vereist dat organisaties vereist dat organisaties zelf een risicobeoordeling uitvoeren en maatregelen nemen om digitale veiligheid en continuïteit te waarborgen.

De meldplicht komt erop neer dat incidenten binnen 24 uur (bij verstoring van dienstverlening) of binnen 72 uur (in andere gevallen) gemeld moeten worden.

Het toezicht bestaat uit proactieve controles voor essentiële entiteiten en reactieve controles na aanleiding voor belangrijke entiteiten. Wanneer de wet niet wordt nageleefd kunnen er boetes worden opgelegd. Bestuurders zijn persoonlijk verantwoordelijk en hoofdelijk aansprakelijk voor het voldoen aan de NIS2 richtlijn.

NIS2

Eind 2024 wordt de tweede Network and Information Security (NIS2) richtlijn van kracht. De wetgeving hiervoor is nog in ontwikkeling, maar het is verstandig om voorbereid te zijn. Want organisaties die geraakt worden door NIS2 moeten voldoen aan de wetgeving zodra deze van kracht wordt.

Daarnaast is het zo dat alle organisaties in Nederland zelf moeten bepalen of ze aan NIS2 moeten voldoen. Iedereen moet dus actie ondernemen!

Belangrijke links

De website van het **Nationaal Cyber Security Centrum** (NCSC): https://www.ncsc.nl

Actuele NIS2-informatie van het NCSC:
NIS2-richtlijn

NIS2 Zelfevaluatie: online vragenlijst om vast te stellen of NIS2 van toepassing is op uw organisatie

De weg naar NIS en NIS2

2013

Publicatie EU Cybersecurity Strategie

2016

Network and Information Security richtlijn goedgekeurd. In Nederland is deze opgenomen in de Wet Beveiliging Netwerk- en Informatiesystemen (WBNI)

2019

EU-lidstaten moeten Computer Security Incedent Response Teams (CSIRTs) oprichten en informatie delen met het Europees Agentschap voor Cybersecurity (ENISA)

2022

NIS2-richtlijn vastgesteld

2023

Januari: start implementatietermijn van 21 maanden. Dwz: de richtlijn moet worden omgezet in wetgeving per lidstaat

2024

Eind 2024 treedt de wetgeving die de NIS2-richtlijn implementeert in werking. Vanaf dat moment moeten organisaties die onder de NIS2-richtlijn vallen, voldoen aan de wet

Wat is NIS2?

NIS2 is de opvolger van de oorspronkelijke NIS-richtlijn uit 2018. NIS2 is de nieuwe Europese richtlijn voor netwerk- en informatiebeveiliging en treedt in oktober 2024 in werking. Het doel van NIS2 is tweeledig. Enerzijds om meer Europese harmonisatie te bereiken. Anderzijds is het doel om een hoger niveau van cybersecurity onder bedrijven en organisaties te bevorderen. Waar de oorspronkelijke NIS-richtlijn zich concentreerde op essentiële sectoren, zoals water, energie en telecom, gaat NIS2 meer organisaties raken.

Nederland werkt aan de doorvertaling van deze richtlijn en daarbij is het Nationaal Cyber Security Centrum (NCSC) betrokken. Dit is het expertisecentrum voor cybersecurity in Nederland.

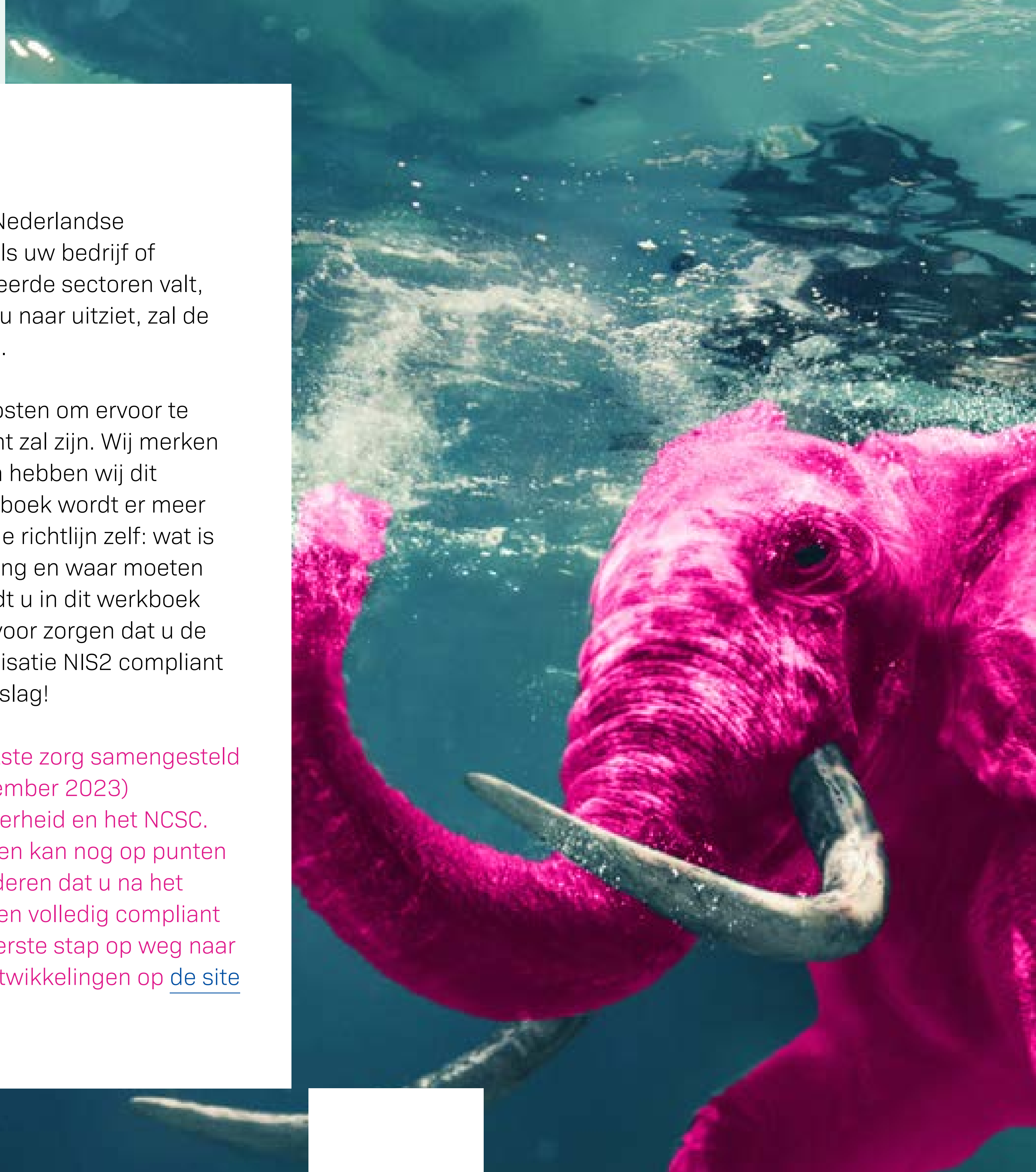
"De afgelopen jaren zien we dat diverse ontwikkelingen in toenemende mate de veiligheid van onze maatschappij en economie onder druk zetten. Denk daarbij aan COVID-19, de oorlog in Oekraïne, en cyberdreigingen. In het licht van deze ontwikkelingen is er sinds 2020 vanuit de Europese Unie gewerkt aan de Network and Information Security (NIS2) directive. Deze richtlijn is gericht op een verbetering van de digitale en economische weerbaarheid van Europese lidstaten." (NCSC.nl)

Wat is de urgentie?

NIS2 is belangrijke wetgeving waar alle Nederlandse organisaties door geraakt worden. Ook als uw bedrijf of organisatie niet in de door NIS2 gedefinieerde sectoren valt, moet u actie ondernemen. Zoals het er nu naar uitziet, zal de NIS2-richtlijn vanaf oktober 2024 gelden.

Dit lijkt ver weg maar het gaat veel tijd kosten om ervoor te zorgen dat uw organisatie NIS2 compliant zal zijn. Wij merken dat er veel vragen zijn over NIS2. Daarom hebben wij dit NIS2-werkboek ontwikkeld. Met dit werkboek wordt er meer informatie gegeven over de inhoud van de richtlijn zelf: wat is NIS2, voor wie is de richtlijn van toepassing en waar moeten organisaties aan voldoen. Daarnaast vindt u in dit werkboek ook een stappenplan en checklist die ervoor zorgen dat u de eerste stappen kunt zetten om uw organisatie NIS2 compliant te krijgen. U kunt hier direct mee aan de slag!

Disclaimer: dit document is met de grootste zorg samengesteld aan de hand van de op dit moment (november 2023) beschikbare informatie vanuit de Rijksoverheid en het NCSC. Maar de wetgeving is nog niet afgerond en kan nog op punten wijzigen. We kunnen dan ook niet garanderen dat u na het doorlopen van de hier beschreven stappen volledig compliant zal zijn. Dit werkboek doorlopen is een eerste stap op weg naar compliancy. Blijf op de hoogte van de ontwikkelingen op de site van het NCSC.



De NIS2 verplichtingen

NIS2 gaat naar verwachting drie verschillende verplichtingen benoemen:

Zorgplicht

De NIS2-richtlijn bevat een zorgplicht die entiteiten verplicht zelf een risicobeoordeling uit te voeren, op basis waarvan zij passende maatregelen nemen om hun diensten zoveel mogelijk te waarborgen en de gebruikte informatie te beschermen.

Meldplicht

De NIS2-richtlijn schrijft voor dat entiteiten incidenten binnen 24 uur moeten melden bij de toezichthouder. Het gaat om incidenten die de verlening van de essentiële dienst aanzienlijk (kunnen) verstoren. In het geval van een cyberincident moet het ook gemeld worden bij het Computer Security Incident Response Team (CSIRT). Zij kunnen vervolgens hulp- en bijstand leveren. Factoren die een incident meldingswaardig maken zijn bijvoorbeeld: het aantal personen dat door de verstoring is geraakt, de tijdsduur van een verstoring en de mogelijke financiële verliezen.

Toezicht

Organisaties die onder de richtlijn vallen komen ook onder toezicht te staan, waarbij wordt gekeken naar de naleving van de verplichtingen uit de richtlijn, zoals de zorg- en meldplicht.

Voor wie gaat NIS2 gelden?

Een verschil met de oorspronkelijke NIS2-richtlijn, is dat bedrijven die in bepaalde sectoren opereren en voldoen aan bepaalde criteria automatisch onder de NIS2-richtlijn vallen. De tweede NIS-richtlijn deelt organisaties in op basis van hun sectoren en hun belang voor de samenleving en economie. Deze zijn onderverdeeld naar 'Essentiële Entiteiten' en 'Belangrijke Entiteiten'. Daarnaast zijn er nog de bijzondere gevallen, zoals ketenpartners van deze twee soorten entiteiten.

Tabel A: Essentiële Entiteiten

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

Tabel B: Belangrijke Entiteiten

Digitale aanbieders	Post- en koeriersdiensten	Afvalstoffen beheer	Levens-middelen
Chemische stoffen	Onderzoek	Vervaardiging/ maakindustrie	

Classificatie

Op basis van deze twee tabellen hanteert NCSC de volgende classificatie om te bepalen of NIS2 van toepassing is op uw organisatie:

Essentiële entiteiten: Grote organisaties in sectoren van tabel A, met meer dan 250 werknemers of een omzet van meer dan 50 miljoen euro en een balanstotaal van meer dan 43 miljoen euro. Zij worden gezien als vitale onderdelen van onze economie en maatschappij en worden proactief gemonitord door de overheid.

Belangrijke entiteiten: Middelgrote organisaties in sectoren van tabel A en middelgrote tot grote organisaties in sectoren van tabel B. Deze hebben minstens 50 werknemers of een jaaromzet en balanstotaal van meer dan 10 miljoen euro. Zij vallen onder een minder strikt toezicht regime en kunnen audits verwachten als er aanwijzingen voor niet-naleving van de wet zijn of als er een incident heeft plaatsgevonden.

Hiernaast zullen nog meer organisaties moeten voldoen aan NIS2:

- Specifieke kleine organisaties
- Ketenpartners
- Uitzonderingen

Bijzondere gevallen

Specifieke kleine organisaties: Hoewel zij doorgaans niet onder de NIS2-richtlijn vallen, kunnen bepaalde micro- en kleine bedrijven die essentiële diensten leveren of op bepaalde gebieden actief zijn, toch onder de richtlijn vallen. Dit geldt met name voor aanbieders van specifieke digitale diensten en bepaalde overheidsinstanties. Denk hierbij bijvoorbeeld aan organisaties die een belangrijke rol hebben bij het functioneren van de infrastructuur van het internet.

Ketenpartners: organisaties die op zich zelf niet onder de NIS2 richtlijn vallen, zullen toch moeten voldoen aan de eisen wanneer ze onderdeel zijn van het kernproces van de toeleveringsketen van een essentiële of belangrijke organisatie. Het is dus ook van belang voor uw organisatie of uw klanten of partners onder de NIS2 richtlijn vallen!

Uitzonderingen: de overheid kan specifieke organisaties aanwijzen die in geen van de hierboven genoemde categorieën passen, maar toch moeten voldoen aan de NIS2 richtlijn.

Handhaving

NIS2 wordt wettelijk verplicht en alle organisaties die in de genoemde categorieën vallen plus de genoemde bijzonder gevallen moeten hieraan voldoen vanaf het moment dat de wet van kracht wordt.

Er zal ook actief worden gecontroleerd op de naleving van de wet. Alle essentiële entiteiten zullen proactief steeksproefsgewijs worden gecontroleerd. Zij zullen dus op elk moment moeten kunnen bewijzen dat ze aan de wet voldoen.

Voor de belangrijke entiteiten gelden reactieve controles. Zij zullen pas aan moeten tonen dat ze aan de wet voldoen na een duidelijke aanleiding. Dit laatste zal in de praktijk vaak neerkomen op een (stevig) cyberincident.

De wet wordt automatisch van toepassing

Wanneer uw organisatie actief is in een van de genoemde categorieën of ketenpartner is, dan moet u automatisch voldoen aan de wet. (De specifieke kleine organisaties en uitzondering worden aangewezen door de overheid. Het automatisme is daar dus niet van toepassing). Dit is anders dan met de eerste versie van NIS, want daarin wordt een organisatie door het ministerie aangewezen.

Boetes

Als na controle blijkt dat een organisatie niet voldoet aan de wet die NIS2 regelt, dan kan er een boete worden opgelegd door de toezichthouder. De lidstaten mogen zelf de hoogte van de boetes vaststellen. De maximale boetes zijn als volgt:

- Voor essentiële organisaties: tot 10 miljoen euro of 2% van de wereldwijde jaaromzet
- Voor belangrijke organisaties: tot 7 miljoen euro of 1,4% van de wereldwijde jaaromzet.

Hoofdelijke aansprakelijkheid

Alle bestuurders zijn persoonlijk verantwoordelijk en aansprakelijk voor het voldoen aan de NIS2 richtlijn. Niemand kan zich verschuilen achter de beslissingen of nalatigheid van een ander.

Voorbereiden op NIS2

De Rijksoverheid en het NCSC hebben een zelfevaluatie en diverse basismaatregelen opgesteld waarmee u nu al mee aan de slag kunt. Dit wordt uitgewerkt in onderstaande stappenplan. Nogmaals: er wordt nog gewerkt aan de NIS2 wetgeving, dus deze maatregelen kunnen nog wijzigen!

Stap 1: Is NIS2 van toepassing?

De Rijksoverheid heeft in oktober 2023 een online zelfevaluatie opgezet. Met deze zelfevaluatie bepaalt u voor uw organisatie:

1: Is de NIS2-richtlijn van toepassing op uw organisatie?	2: Is uw organisatie Essentieel of Belangrijk?	3: Valt uw organisatie onder Nederlands toezicht?

De zelfevaluatie bevat gedetailleerde vragen over het soort producten, diensten en omvang van uw organisatie. Klik op deze link om naar de zelfevaluatie tool te gaan van het NCSC.

Valt uw organisatie onder de NIS2-regelgeving? Dan kunt u door met het stappenplan.

Valt uw organisatie NIET onder de NIS2-regelgeving? Dan is het verstandig om de adviezen van het NCSC en de Rijksoverheid in de gaten te blijven houden. Wellicht dat uw organisatie toch nog geraakt gaat worden als de wetgeving zich ontwikkelt. En ook als dit niet zo is, is het verstandig om de basis met betrekking tot online veiligheid toch op orde te hebben.

Stap 2: Basismaatregelen NIS2

	MAATREGEL
1	**Richt risicomanagement in:** Incidenten kunnen een grote impact hebben op organisatiedoelen. Om uw bedrijfsvoering zo ongestoord mogelijk te laten verlopen, wilt u een passend niveau van weerbaarheid realiseren. Een passend niveau wil zeggen dat de maatregelen die u neemt uw organisatie beschermen zonder de bedrijfsvoering te belemmeren of tot onnodige kosten te leiden.
2	**Pas sterke authenticatie toe:** Authenticatie is de techniek waarmee een systeem kan vaststellen wie een gebruiker is. Hiermee krijgt een gebruiker toegang tot gegevens of systemen. Zo zorgt u voor een veilig inlog systeem.
3	**Bepaal wie toegang heeft tot uw data en diensten:** Geef medewerkers alleen toegang tot informatie, systemen en locaties die nodig zijn voor het uitvoeren van hun taak. Dit geldt dus voor zowel logische als fysieke toegang. Dit beperkt de gevolgen van gebruikersfouten die vervelende gevolgen kunnen hebben.
4	**Beperk het aanvalsoppervlak:** De meeste software, computer- en netwerkapparatuur bevatten meer functionaliteit dan een organisatie nodig heeft. Dit kan tot onnodig kwetsbaarheden leiden waar aanvallers misbruik van kunnen maken. Om het aanvalsoppervlak te beperken kunt u een maatregelen nemen zoals hardening en segmentering.
5	**Gebruik versleuteling:** Het versleutelen van al uw bedrijfsinformatie maakt data onbruikbaar als deze in handen van aanvallers valt.
6	**Bescherm uw organisatie tegen verlies van gegevens:** Om uw organisatie te beschermen tegen het verlies van data als er toch iets misgaat, dient u een back-up beleid te hebben. In het back-up beleid worden de eisen meegenomen die u stelt aan het bewaren en beschermen van uw data. Deze eisen stelt u mede vast op basis van een risicoafweging.
7	**Maak back-ups:** Bedenk van welke data back-ups noodzakelijk zijn en hoelang u deze moet bewaren. Test het terugzetten van uw back-ups zodat u zeker weet dat uw bedrijfsvoering bij dataverlies maar beperkt wordt verstoord. Oefen het recovery-proces met medewerkers die dergelijke werkzaamheden in de praktijk moeten kunnen uitvoeren.
8	**Richt patchmanagement in:** Leveranciers brengen updates uit om kwetsbaarheden in hun software te verhelpen. Door een patchmanagementproces in te richten, zorgt u dat er een proces is om updates voor uw software te identificeren, te testen en te installeren.
9	**Centraliseer en analyseer loginformatie:** Logbestanden spelen een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Door te zorgen dat applicaties en systemen voldoende loginformatie genereren, voorziet u uzelf van voldoende informatie.

Stap 3: Beleid, processen en procedures

Het implementeren van de nieuwe NIS2-richtlijn kan een uitdaging worden. NIS2 heeft namelijk veel impact op de organisatie. Het betreft niet alleen de technologie, maar ook het interne beleid, procedures en processen binnen de organisatie. Daarom is het verstandig om op tijd te beginnen met het treffen van voorbereidingen. Oktober 2024 lijkt nog best ver weg, maar uit ervaring weten wij dat het optimaal inrichten van beveiliging tijdrovend kan zijn.

Om het u gemakkelijker te maken hebben wij een checklist ontwikkeld die u helpt om het huidige beleid, processen en procedures in kaart te brengen en deze voor te bereiden op de NIS2-regelgeving. De checklist uit stap 2 is vooral gericht op de technische verbeteringen. Zoals eerder al benoemd heeft NIS2 ook grote impact op het interne beleid, processen en de procedures.

Nadat u de basismaatregelen uit stap 2 heeft uitgevoerd is het daarom ook handig om de checklist hiernaast te volgen. Zo zet u ook de eerste stappen om uw beleid, processen en procedures voor te bereiden op NIS2.

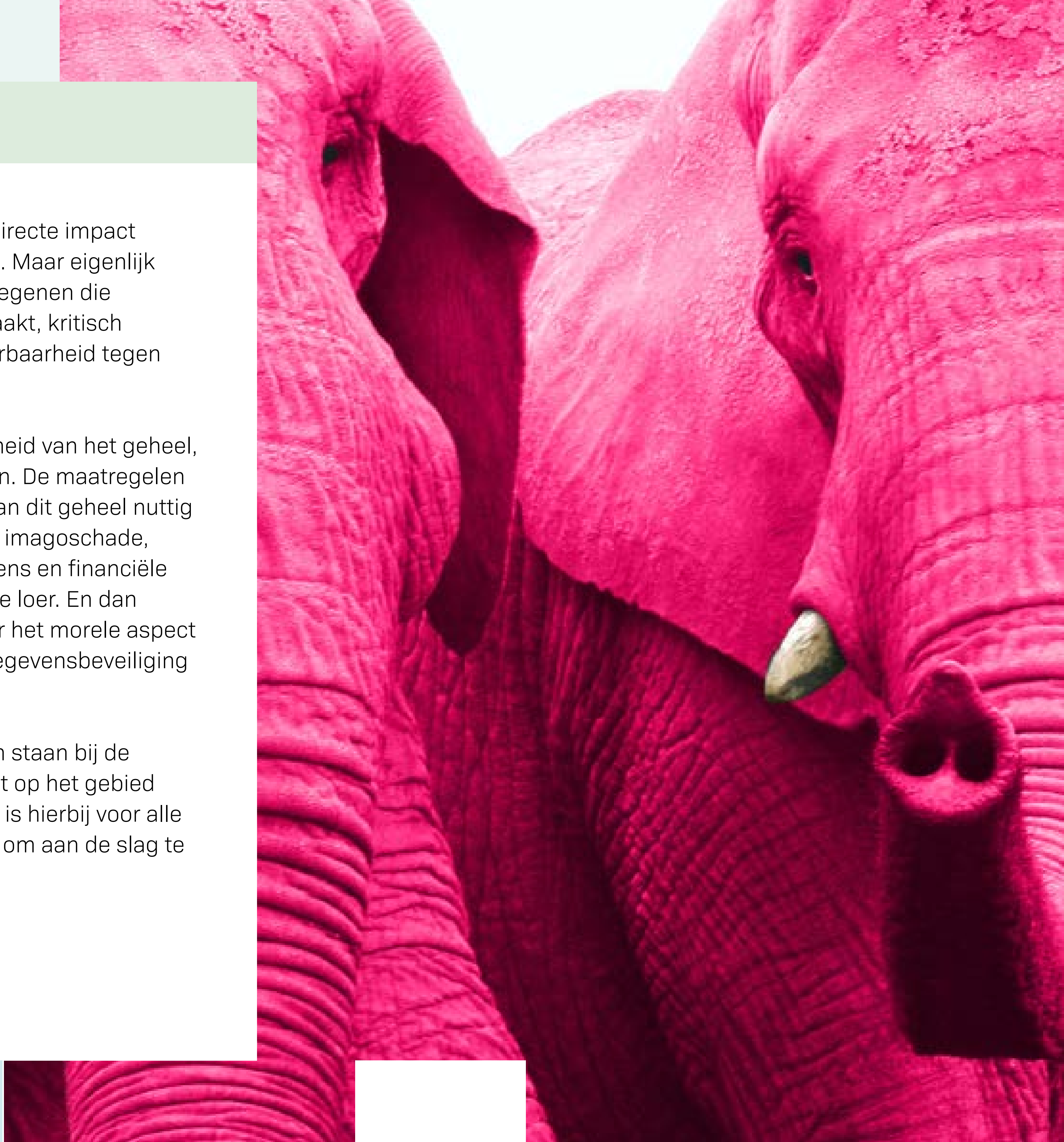
	Activiteit
1	**Risicoanalyse:** De eerste stap is om na te gaan welke systemen en diensten van uw organisatie het meest belangrijk en daarmee het grootste risico lopen bij een hack. Hoe is de beveiliging van deze omgeving ingericht?
2	**Bedrijfscontinuïteit:** Is er een goede back-up, een noodherstel plan en crisisbeheer?
3	**Supply chain security:** Welke potentiële risico's loopt uw organisatie via externe leveranciers en dienstverleners?
4	**Beveiliging van netwerk- en informatiesystemen:** Hoe zijn deze ingericht en hoe wordt er omgegaan met kwetsbaarheden?
5	**Incidentenafhandeling:** Hoe worden incidenten nu afgehandeld en mogelijk geregistreerd?
6	**Doeltreffendheid:** Hoe is het met beleid en de procedures om de doeltreffendheid van cybersecurity te toetsen?
7	**Training:** Hoe goed is iedereen op de hoogte van het computerbeleid binnen de organisatie en wordt die ook nageleefd?
8	**Cryptografie en encryptie:** Hoe zit het met beleid en procedures rondom het gebruik van cryptografie en encryptie?
9	**Fysieke beveiliging:** Van personeel, toegangscontrolebeleid en activabeheer.
10	**Multifactor authenticatie:** Pas die toe bij accounts die vanaf het internet bereikbaar zijn, beheerrechten hebben en op accounts van essentiële systemen.

Tenslotte

De komende NIS2 richtlijn heeft directe impact op veel organisaties in Nederland. Maar eigenlijk zou iedere organisatie, dus ook degenen die niet direct door NIS2 worden geraakt, kritisch moeten kijken naar de eigen weerbaarheid tegen cyberbedreigingen.

NIS2 is bedoeld om de weerbaarheid van het geheel, de EU en Nederland, te verbeteren. De maatregelen zijn echter voor alle onderdelen van dit geheel nuttig en praktisch 'best practice'. Want imagoschade, diefstal van vertrouwelijke gegevens en financiële schade liggen voor iedereen op de loer. En dan hebben we het nog niet eens over het morele aspect van een fatsoenlijke basis voor gegevensbeveiliging en dergelijke.

Iedere organisatie zou stil moeten staan bij de eigen weerbaarheid en veerkracht op het gebied van cybersecurity. De komst NIS2 is hierbij voor alle organisaties een goed beginpunt om aan de slag te gaan en te blijven.



Kunnen we helpen?

Hoe kan Pink Elephant helpen?

Pink Elephant heeft een uitgebreid portfolio op het gebied van security. We bundelen deze diensten onder de noemer PinkSecure. U kunt hier meer lezen over PinkSecure.

Een belangrijk onderdeel van PinkSecure is het PinkSOC: ons eigen Security Operations Center in Naarden. Een SOC speelt een belangrijke rol bij de snelle detectie van pogingen om binnen te dringen in uw IT-omgeving. Lees hier meer over het PinkSOC.

Een veilige en actuele backup van uw bedrijfsgegevens is essentieel om weerbaar te zijn tegen cybersecurity aanvallen. Lees hier meer over de mogelijkheden.

Samen met Microsoft kunen we een volledig assessment uitvoeren op uw IT-infrastructuur. Het resultaat is een overzicht met alles wat goed ingericht en wat beter kan en moet. Lees hier meer over het Security Assessment.

Ook verzorgen we Security Awareness trainingen voor uw medewerkers. Daar kunt u hier meer over lezen

Ons zusterbedrijf True geeft inzicht in de risico's van webapplicaties en websites met een Security Audit door ethische hackers. Lees hier meer over de Security Audit van True.

En net als de wetgeving om NIS2 te verankeren in de Nederlandse wet die nog in ontwikkeling is, zijn we bij Pink Elephant bezig met de verdere ontwikkeling van diensten rondom NIS2. Daarom hebben we daar een aparte webpagina voor gemaakt met een actueel overzicht van de diensten van Pink zelf en onze zusterbedrijven in The Digital Neighborhood.

The Digital Neighborhood

PINK

Pink Elephant maakt IT persoonlijk