WHITEPAPER

Wat betekent NIS2 voor uw organisatie?

Orbid
A RICOH Company

Het aantal cyberaanvallen en -incidenten kent de laatste jaren een flinke stijging. Deze stijging zorgt voor een **hoge druk** op onze economie en samenleving. Zeker omdat we - mede door **externe factoren** zoals COVID-19 - nog afhankelijker zijn van een goed werkende (digitale) infrastructuur.

Om de **cybersecurity in Europa te verscherpen** én de **digitale en economische weerbaarheid** van Europese lidstaten te versterken, heeft de Europese Unie de '**Network and Information Security Directive**' - afgekort NIS2 - goedgekeurd. Via deze nieuwe NIS2-richtlijn wil de EU de **continuïteit van (zeer) kritieke diensten** garanderen aan zijn inwoners.

In deze whitepaper geven we u graag een antwoord op volgende vragen:

- Wat houdt de nieuwe NIS2-richtlijn in?
- Welke organisaties vallen onder de nieuwe wetgeving?
- Welke sancties kan u krijgen indien uw organisatie niet compliant is?
- Welke minimale security maatregelen moet uw organisatie nemen?
- Hoe kan Orbid u ondersteunen in het traject naar NIS2?

NIS2 — Orbid

A RICOH Company

Inhoudstafel

NIS2, de opvolger van NIS1

NIS staat voor **Network and Information Systems** en buigt zich over de beveiliging van netwerkinformatie systemen. Met deze richtlijn wil Europa:

- Het **risico op hacking verminderen** door de juiste maatregelen te nemen.
- De **gevolgen** bij een hacking **beperken** door te zorgen voor goede backups en een snel recovery proces.
- Het **overleg en de samenwerking** op Europees niveau **verbeteren** zodat lidstaten sneller acties kunnen ondernemen.

Om toe te lichten wat NIS2 precies is, keren we even terug naar het ontstaan van de NIS-richtlijn.

2013

De Amerikaanse overheid geeft de opdracht aan het National Institute for Standardization & Technology (NIST) om cybersecurity maatregelen uit te werken waar de belangrijke dienstverleners in Amerika aan moeten voldoen.

2016

Net zoals in Amerika, start de Europese Unie met een plan rond cybersecurity maatregelen. Deze publiceren ze in een eerste wettekst.

2019

België zet de Europese wet om in een Belgische wet waar **7 vitale sectoren**, de zogenaamde 'aanbieders van essentiële diensten', onder vallen.

De NIS-richtlijn is een stap in de goede richting, maar mede door externe factoren zoals COVID en cyberoorlogen zijn er enkele **beperkingen**:

- × Het aantal sectoren is te beperkt.
- × Er is weinig uniformiteit tussen de Europese landen op het vlak van uitwerking en invoering.
- × Er is een gebrek aan informatie-uitwisseling op op Europees niveau.

2022

Om deze beperkingen op te lossen, maakt de EU een **tweede versie**: de NIS2-richtlijn.

- ✓ Meer sectoren
- ✓ Meer uniformiteit voor de deelstaten
- ✓ Verantwoordelijkheden en bevoegdheden
- ✓ Sancties voor bedrijven die de maatregelen niet volgen
- ✓ Verplichte incidentmelding
- ✓ Nauwere samenwerking tussen de landen dankzij een response team (CSIRT)

17 oktober 2024

De NIS2-richtlijn moet tegen 17 oktober 2024 omgezet zijn naar een Belgische wet. Bedrijven die onder de NIS2-wet vallen, moeten tegen deze datum ook **in orde zijn met de verschillende security maatregelen**.

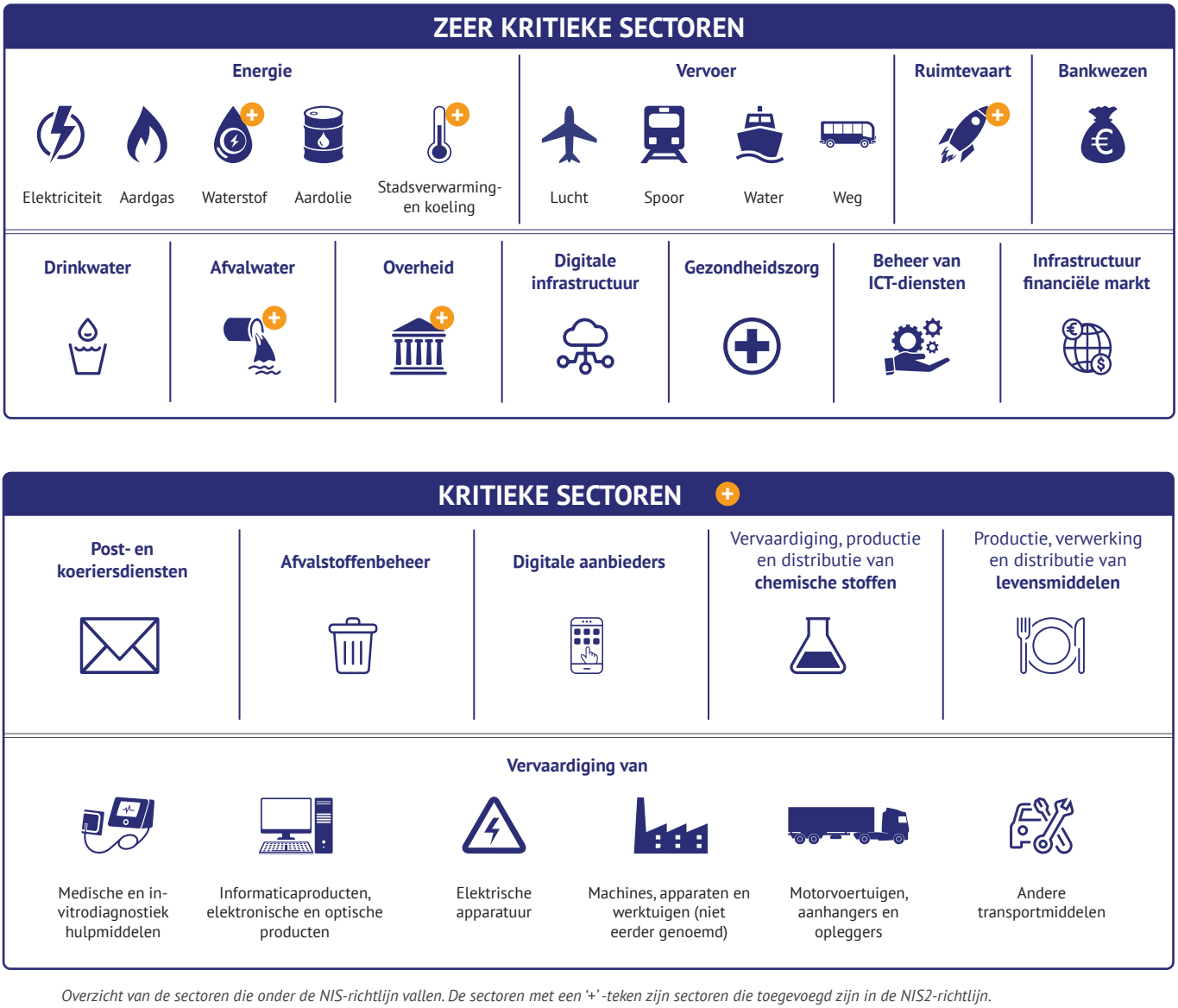
Valt uw organisatie onder NIS2?

Valt uw organisatie onder de NIS2 en zo ja, onder welk beveiligingsniveau? Om dit te bepalen, moet u rekening houden met drie parameters: de **kriticiteit van de sector** waarin uw organisatie actief is, de **diensten en/of activiteiten** die uw organisatie aanbiedt en de **grootte van uw organisatie.**

De combinatie van de sector en de grootte/omzet van uw organisatie zal uw **beveiligingsniveau** (essentieel vs belangrijk) bepalen. Dit niveau heeft invloed op **welke maatregelen** waaraan uw organisatie moet voldoen en welke **maturiteitsscore** uw organisatie moet behalen.

De kriticiteit van de sector

Zoals we eerder al vermeldden, heeft de EU in de NIS2-richtlijn **extra sectoren** opgenomen die compliant moeten zijn. Vroeger vielen instanties in de publieke sector bijvoorbeeld niet onder de wetgeving, terwijl dit nu wel het geval zal zijn. In onderstaande *infographic* vatten we de opdeling tussen zeer kritieke en kritieke sectoren samen:



Overzicht van de sectoren die onder de NIS-richtlijn vallen. De sectoren met een '+' -teken zijn sectoren die toegevoegd zijn in de NIS2-richtlijn.

De diensten en/of activiteiten die uw organisatie aanbiedt

Afhankelijk van de diensten en/of activiteiten die uw organisatie aanbiedt, kan er **een verschil** zijn onder welk **beveiligingsniveau** uw organisatie valt. Zo zal elk bedrijf dat DNS-diensten aanbiedt - onafhankelijk de grootte - vallen onder het niveau 'Essential', terwijl bijvoorbeeld kleine datacenterbedrijven zelfs niet in de scope zijn opgenomen.

De grootte van uw organisatie

Een laatste parameter is de grootte van de organisatie. Het Centrum voor Cybersecurity België (CCB) onderscheidt hierin **drie type organisaties**:

Groot

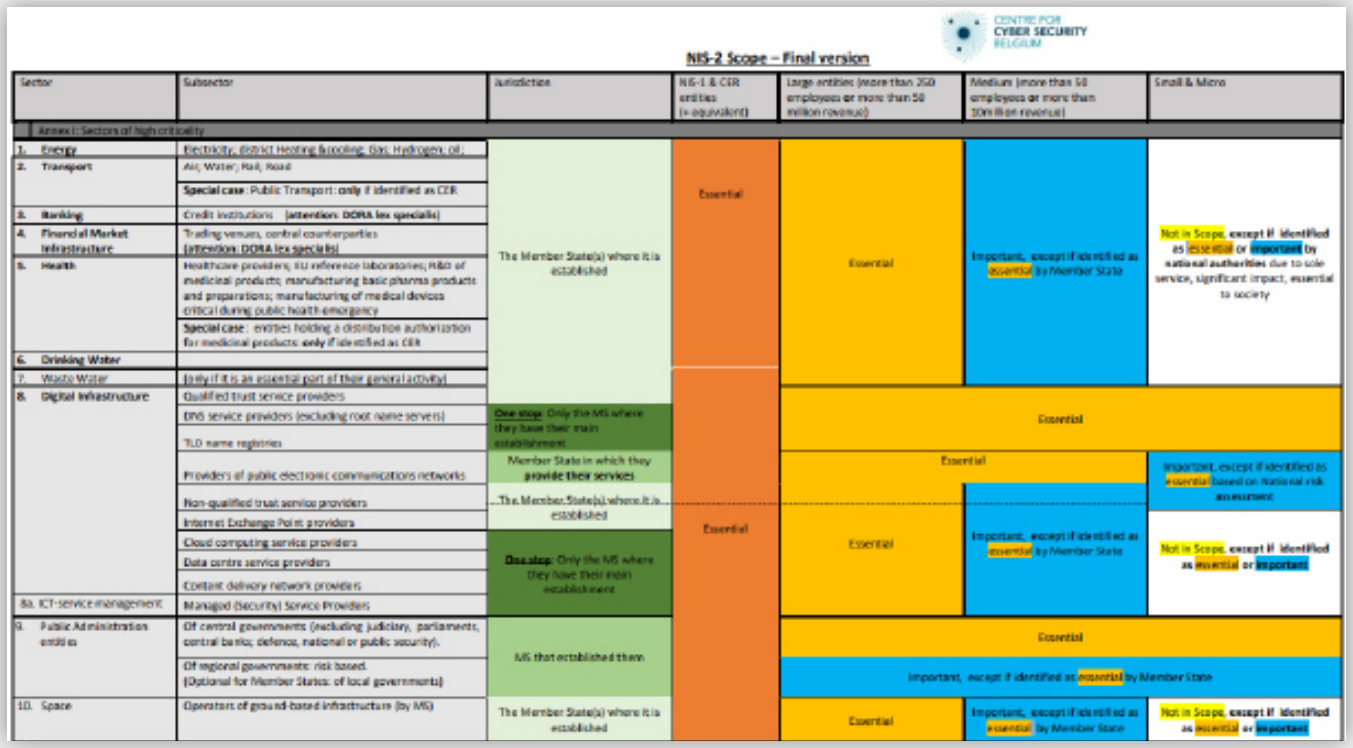
Meer dan 250 medewerkers
OF
Meer dan € 50 miljoen omzet

Middelgroot

Meer dan 50 medewerkers
OF
Meer dan € 10 miljoen omzet

Klein & micro

Maximum 10 medewerkers
OF
Maximum € 2 miljoen omzet



*Voorbeeld van de scope voor NIS2 voor **zeer kritieke sectoren**. De kritieke sectoren zijn in bovenstaande afbeelding niet opgenomen.*

Het CCB kan van deze lijst afwijken. Zo kan het sectoren of bedrijven die volgens de lijst 'out-of-scope' zijn, toch maatregelen opleggen waardoor die moeten voldoen aan 'Essential' of 'Important'.

Orbid
A RICOH Company

De toeleveranciers (supply chain)

De recente wijzigingen in de NIS-wetgeving hebben niet alleen geleid tot de toevoeging van extra sectoren, maar omvatten ook de toeleveringsketen. Met andere woorden, zelfs als uw organisatie **'out-of-scope'** is, kan het voorkomen dat uw **klanten van u verlangen dat u voldoet aan de essentiële of belangrijke maatregelen van NIS2**. Zeker voor openbare aanbestedingen kan dit grote gevolgen hebben.

Kortom: zo goed als elk bedrijf zal maatregelen moeten nemen.

Meer weten over NIS2?

Bij Orbid beschikken we over verschillende experten voor NIS2. Hebt u een vraag of wenst u ondersteuning? Wij helpen u graag verder.

Welke verplichtingen hebt u?

Welke maatregelen u als organisatie precies moet nemen, hangt af van hoe België de wet precies zal uitvoeren. Net zoals er per sector afwijkingen mogelijk zijn of u al dan niet onder NIS2 valt, kan België ook strengere maatregelen invoeren in vergelijking met het 'Europese minimum'.

De Europese Unie legt in artikel 21 **tien minimale cybersecurity maatregelen** op waar elke organisatie die onder de NIS2-wet valt aan moet voldoen.

1 Een beleid rond **risicoanalyse** en de **beveiliging** van **informatiesystemen**

Uw organisatie is verplicht om een **information security policy** (informatieveiligheidsbeleid) te hebben. In dit document lijst u alle mogelijke aspecten op die een gevaar of schade kunnen vormen voor uw organisatie.

2 **Incidenten-** en **crisisbeheer**

Bent u voorbereid op incidenten? Welke procedures en verantwoordelijkheden zijn er binnen uw organisatie in het geval van een ramp? Welke maatregelen treft u voor, tijdens en na een incident?

Als organisatie moet u een **duidelijk incident response plan** hebben waarin u alle stappen en verantwoordelijkheden toelicht.

3 Garantie voor de **bedrijfscontinuïteit**

Uw organisatie moet de bedrijfscontinuïteit kunnen garanderen, ook als u te maken krijgt met een eventueel disaster. Zorg ervoor dat u een **duidelijk backup en business continuity plan** hebt. Neem regelmatig goede **backups** en voer ook **recovery testen** uit op uw cruciale data.

4 Garantie en beveiliging van de **continuïteit van uw supply chain**

Zoals eerder vermeld in de whitepaper moet uw organisatie ervoor zorgen dat uw toeleveringsketen ook voldoet aan een bepaald beveiligingsniveau. Zo kan u uw leveranciers ertoe verplichten om aan te tonen dat ze **voldoen aan de maatregelen**. Anderzijds kunnen uw klanten dit ook vragen aan uw organisatie. Het aantonen kan door de vragenlijst van de CCB in te vullen en deze door te sturen.

5 Beveiliging bij het **verwerven, ontwikkelen en onderhouden** van netwerk- en informatiesystemen

NIS2 verplicht uw organisatie om snel actie te ondernemen bij eventuele kwetsbaarheden en deze ook meteen te patchen. Een **goed patch en vulnerability management** en de **juiste technische maatregelen** voor alle security lagen zijn dan ook cruciaal.

6 Beleid en procedures om de **effectiviteit van de maatregelen** te beoordelen

Organisaties die onder NIS2 vallen, moeten een **evaluatiebeleid en -procedures** implementeren om te garanderen dat de genomen veiligheidsmaatregelen ook effectief zijn. Dit omvat zowel **interne als externe audits**, waaronder ethical hacking. Doe ook regelmatig checks waar u ziet wie toegang heeft tot uw IT-omgeving, welke medewerkers MFA gebruiken en welke accounts al 30 dagen niet meer hebben ingelogd.

7 Basispraktijken voor **cyberhygiëne**

Zorg voor een basiscursus cybersecurity voor huidige én nieuwe medewerkers. Via een **security awareness aanpak** maken uw medewerkers kennis met de laatste cybertechnieken die criminelen toepassen en krijgen ze duidelijke tips om zich beter te beveiligen in de digitale wereld.

8 Beleid & procedures voor **cryptografie en encryptie**

Implementeer een beleid en creëer procedures voor het gebruik van cryptografie, waaronder encryptie. Installeer tools zoals **BitLocker** op alle apparaten en gebruik HTTPS met officiële certificaten voor uw website(s). Met een doordacht encryptiebeleid kunt u uw digitale bescherming verbeteren.

9 Beveiligingsaspecten ten aanzien van **personeel, toegangsbeleid en beheer van activa**

Zorg ervoor dat medewerkers **strikte beveiligingsprocedures** volgen wanneer ze toegang hebben tot gevoelige gegevens. Kies voor een uitgebreid beleid rond fysieke en gegevenstoegang en neem dit ook mee in documenten die u aan medewerkers bezorgt. Maak daarnaast ook een **inventaris op van alle bedrijfsmiddelen** en zorg ervoor dat uw medewerkers deze correct gebruiken.

10 Gebruik **Multifactor Authenticatie (MFA)** wanneer gepast

Gebruik Multifactor Authenticatie **voor al uw toepassingen**: vpn, Citrix, Microsoft 365,... In artikel 21 staat er 'wanneer gepast', waarmee het CCB doelt op gevoelige data zoals financiële of medische data. Bij Orbid raden we echter aan om Multifactor Authenticatie altijd te implementeren omdat het een groot deel van de cyberaanvallen kan afwenden.

Via onze oplossingen kunnen we uw organisatie optimaal ondersteunen in de transitie naar NIS2. Meer informatie hierrond vindt u vanaf pagina 16 van deze whitepaper.

Orbid A RICOH Company

Toezicht op de NIS2-wetgeving

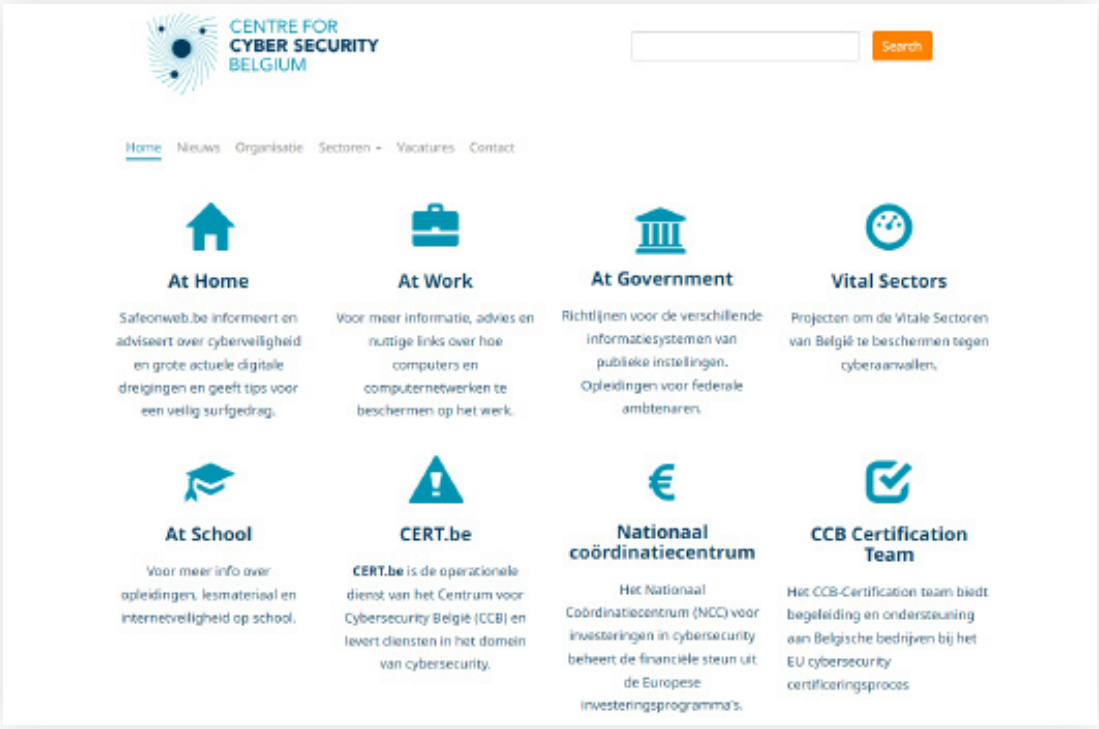
Het **Centrum voor Cybersecurity in België (CCB)** is verantwoordelijk voor de supervisie rond NIS2. Zij moeten toezicht houden op de bedrijven zodat ze de wet naleven. Maar bent u verplicht elk cyberincident te melden? Welke controles kan u krijgen indien uw organisatie onder NIS2 valt? En welke sancties kan het CCB uw organisatie opleggen indien u niet compliant bent?

Meldingsplicht

Net zoals bij de GDPR-wetgeving die in 2018 in werking trad, is er voor NIS2 ook een meldingsplicht voor **significante incidenten**.

> ### Wat is een significant incident?
>
> Een significant incident is een incident die zorgt voor een ernstige **operationele verstoring**, sterke financiële verliezen of (im)materiële schade berokkent aan inwoners.

Bovenstaande verduidelijken we graag met een voorbeeld. Een poging tot phishing is een niet-significant incident want er is geen ernstige operationele verstoring. Is uw organisatie slachtoffer van een cyberaanval waardoor u enkele dagen niet kan werken, dan bent u verplicht dit te melden aan het CCB. Zijn er bovendien ook persoonsgegevens betrokken, dan moet u het **zowel melden bij het CCB als bij de Gegevensbeschermingsautoriteit (GBA)**.



Website van het CCB waar u handige links terugvindt naar CERT, het Nationaal Coördinatiecentrum en meer. (https://ccb.belgium.be/nl)

Waar u bij GDPR de eerste melding binnen de 72 uur moest indienen, is de CCB voor NIS2 strenger. Doet er zich een significant incident voor bij uw organisatie, dan moet u dit via het CERT-meldingsformulier melden **binnen de 24 uur.** Binnen de **72 uur** moet u de melding hebben aangevuld met de **details**. Daarnaast moet u na ten laatste **een maand na het incident** ook een **eindverslag** indienen waarin u gedetailleerd omschrijft wat er gebeurd is, welke risicobeperkende maatregelen u hebt genomen en wat de gevolgen zijn.

Toezicht en sancties

Onder welk toezicht uw organisatie valt en welke sancties het CCB uw organisatie kan opleggen indien u niet wil voldoen aan de maatregelen, hangt af van het beveiligingsniveau van uw organisatie.

	Toezicht	Sancties*
Essentiële entiteiten	**Proactief** toezicht Het CCB kan uw organisatie verzoeken bepaalde informatie te bezorgen of kunnen ter plaatse komen om een audit af te nemen.	**Administratieve boetes** tot maximum 10 miljoen euro of 2% van de jaaromzet van uw organisatie. In zeer extreme gevallen kan het CCB ook het certificaat intrekken en/of een verbod opleggen voor de CEO voor het uitvoeren van zijn/haar functie gedurende een aantal maanden.
Belangrijke entiteiten	**Reactief** toezicht Deed er zich een incident voor en hebt u dit (niet) gemeld, dan kan het CCB informatie opvragen aan uw organsiatie en indien nodig ter plaatse een audit uitvoeren om te kijken of u met alles in orde bent.	**Administratieve boetes** tot 7 miljoen euro of 1,4% van de jaaromzet.

* In sommige gevallen kan het CCB ook dwangsommen opleggen.

Praktische uitwerking in België

Eerder in deze whitepaper zeiden we al dat er op Europees vlak twee beveiligingsniveaus zijn vastgelegd: **essentieel en belangrijk**. Toch kan elke lidstaat beslissen om het voorstel van de EU verder uit te werken. Zo heeft het CCB naast essentieel en belangrijk nog twee beveiligingsniveaus toegevoegd in de Belgische richtlijn: **basis en small**. Valt uw organisatie niet onder NIS2, dan adviseert het CCB toch om te voldoen aan het basisniveau.

Het Cyberfundamentals Framework

Het Cyberfundamentals Framework biedt een **overzicht van de maatregelen** die organisaties moeten nemen, afhankelijk van hun beveiligingsniveau. Dit framework in Excel is gebaseerd op het Amerikaanse NIST-framework en omvat **zes categorieën**: Identify, Protect, Detect, Respond, Recover en Governance . Elke categorie bestaat uit een aantal maatregelen en submaatregelen.

Small & micro

Het startniveau 'Small & micro' laat een organisatie toe om een eerste beoordeling te maken. Het is bedoeld voor micro-organisaties zoals een eenmanszaak of organisaties met beperkte technische kennis.

7 must have maatregelen

Basis

Het beveiligingsniveau 'Basis' bevat de standaard informatiebeveiligings-maatregelen voor alle organisaties. Deze bieden een effectieve beveiligingswaarde met technologie en processen die over het algemeen al beschikbaar zijn. Waar nodig zijn de maatregelen aangepast en verfijnd.

40 maatregelen waarvan 13 must have

Belangrijk

Het beveiligingsniveau 'Belangrijk' is ontworpen om de risico's van gerichte cyberaanvallen door personen met standaard vaardigheden en middelen tot een minimum te beperken, naast de bekende cybersecurity risico's.

154 maatregelen waarvan 21 must have
(13 basis must have + 8 must have)

Essentieel

Het beveiligingsniveau 'Essentieel' gaat nog een stap verder en is ontworpen om het risico op geavanceerde cyberaanvallen door personen met uitgebreide kennis en resources te verminderen.

234 maatregelen waarvan 29 must have
(13 basis must have + 8 belangrijke must have + 8 must have)

De 7 must have maatregelen voor kleine & micro-organisaties

Beveilig alle logins met MFA

Bij Orbid adviseren we elke organisatie om **alle toegang van bedrijfsdata** via MFA te beveiligen. Denk zowel aan applicaties binnen Microsoft 365 als uw VPN, Citrix, Remote Desktop Services (RDS),...

Installeer onmiddellijk alle security updates

Zorg ervoor dat u een **goed patch management** hebt, niet alleen van uw servers, maar ook van uw clients zoals laptops en smartphones. Via tools zoals Microsoft 365 Intune kan u uw clients eenvoudig managen, beheren en patchen.

Installeer een goede antivirus

Installeer een **next gen antimalware** of EDR zoals Microsoft Defender for Endpoint die ook abnormaal gedrag kan detecteren.

Beveilig uw netwerk

De meeste bedrijven zullen in orde zijn met hun firewalls. Toch raden we organisaties aan om een stap verder te gaan door bijvoorbeeld **Netwerk Acces Control** zoals Aruba ClearPass te installeren en Remote Access Control te gebruiken om vpn's te beveiligen.

Neem een backup van uw data

Een goede backup van uw data is cruciaal. We adviseren organisaties steeds om een **offline airgapped backup** of **immutable backup** te nemen. Indien hackers er toch in slagen uw netwerk te hacken en uw backups encrypteren, dan hebt u nog steeds een offline versie die u kan terugzetten. Bij Orbid gaan we voor onze immutable backup as a service steeds te werk volgens het '3-2-1-1-0' principe.

Administratierechten

Niemand mag voor dagelijkse taken werken met **administrator rechten**. Om gebruik te maken van extra rechten, moet u inloggen op aparte accounts zoals een admin-account. Evalueer jaarlijks de administrators binnen uw organisatie en verwijder leveranciers die toegang hebben, maar waarmee u niet langer samenwerkt.

Andere aanbevelingen

- Bescherm computers en mobiele toestellen tegen diefstal door gebruik te maken van bv. remote wipe. Binnen Microsoft 365 kan u dit eenvoudig regelen via Microsoft Intune.
- Beperk de (fysieke) toegang tot uw servers en backups.
- Zorg dat u een incidentenplan hebt waarin ook steeds de contactpersonen vermeld staan.

Wist u dat:

Indien u ISO27001 gecertificeerd bent zoals Orbid, dan bent u automatisch ook compliant op het niveau 'Essentieel'. Bovendien kan u via onze **'Managed Modern Workplace'-oplossing via Microsoft** al een sterke beveiligingsbasis leggen om te voldoen aan de vereisten van NIS2.

Orbid A RICOH Company

De NIS2-aanpak van Orbid

Bij Orbid beschikken we over verschillende **experten** die u kunnen ondersteunen bij de transitie naar NIS2, zowel op het vlak van **praktische aanpak** als bij de **implementatie van technische maatregelen**. Om organisaties te helpen, starten we steeds vanuit een 5-stappenplan.

Het 5-stappen plan van Orbid

1) We bekijken of uw sector onder de NIS2-wetgeving valt.

2) We bepalen uw beveiligingsniveau.

3) We bepalen de maturiteit van uw organisatie via onze maturiteitscheck.

4) We maken in samenspraak met de klant een actieplan op en kunnen indien nodig technische implementaties uitvoeren.

5) We zorgen voor een goede borging & evaluatie.

Vragen rond onze NIS2-begeleiding?

Hebt u vragen rond onze NIS2-begeleiding? Contacteer gerust onze experten, wij helpen u graag verder.

1) Valt uw sector onder de NIS2 wetgeving?

Een eerste stap is om te kijken in welke sector uw organisatie werkzaam is en of u in aanmerking komt voor NIS2.

2) Bepaal uw beveiligingsniveau

Via de **CyFun Selection tool** kan u het beveiligingsniveau van uw organisatie bepalen. Eenmaal u de juiste sector en grootte van uw organisatie hebt geselecteerd, kan u de impact en waarschijnlijkheid per cyberaanval categorie en per 'threat actor' controleren. Onderaan rechts ziet u ook meteen aan welk niveau (basis / belangrijk / essentieel) uw organisatie moet voldoen.

CENTRE FOR CYBER SECURITY BELGIUM — Version: 2023-08-24

Manufacturing			Common skills		Common skills		Common skills		Extended Skills		Extended Skills			
Organization Size (L/M/S = 3/2/1)	3	Threat Actor Type	Competitors		Ideologues Hactivists		Terrorist		Cyber Criminals		Nation State actor			
Cyber Attack Category	Global or Targetted	Impact	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score		
Sabotage/ Disruption (DDOS,...)	2	Med	Med	15	Low	0	Low	0	Low	0	Med	15		
Information Theft (espionage, ...)	2	High	High	60	Low	0	Low	0	Med	30	Med	30		
Crime (Ransom attacks)	1	Med	Low	0	Low	0	Low	0	High	15	Med	7,5		
Hactivism (Subversion, defacement...)	1	Low	Low	0	Med	0	Low	0	Low	0	Low	0		
Disinformation (political influencing)	1	Low	Low	0	Low	0	Low	0	Low	0	Low	0	Score	CyFun Level
	Total	Total		75		0		0		45		52,5	172,5	IMPORTANT

Voorbeeld van de CyFun Selection tool.

3) NIS2 maturiteitscheck

Bij Orbid beschikken we over een NIS2 maturiteitscheck waar we via een **gap-analyse** de huidige situatie in kaart brengen. Over welke documenten beschikt u al? Welke documenten moet u nog opmaken? We werken een concreet actieplan uit en kennen prioriteiten toe.

Hebt u bepaalde documenten nog niet opgemaakt? Orbid beschikt over een **50-tal templates** die u kan gebruiken voor NIS2-, GDPR- en ISO27001 compliancy, waaronder:

- Backup plan
- Business Continuity Plan
- Patch management plan
- Anti-malware plan
- Basic Incident Respons Plan
- Asset management
- ICT policy
- Access control policy
- Informatieveiligheidsbeleid

Vraag een NIS2 maturiteitscheck aan

Orbid A RICOH Company

4) Security acties uitvoeren

Eenmaal we de huidige situatie in kaart hebben gebracht en een actieplan hebben opgemaakt, kan Orbid uw organisatie ondersteunen bij het implementeren van de nodige security maatregelen.

Om u hiervan een overzicht te geven, keren we nog even terug naar artikel 21: de **10 minimale cybersecurity maatregelen** die uw organisatie moet nemen.

Een beleid rond risicoanalyse en de beveiliging van informatiesystemen

NIS2-maturiteitscheck

Hebt u bepaalde documenten nog niet opgemaakt? Orbid beschikt over een 50-tal templates die u kan gebruiken voor NIS2-, GDPR- en ISO27001 compliancy, waaronder:

- ICT policy
- Informatieveiligheidsbeleid

Orbid A RICOH Company | Managementsysteem voor Informatiebeveiliging | Auteur: | Versie: | Datum: | Pagina:

1. *Definities*

"ICT": Informatie en Communicatie Technologie.

"Medewerker": Arbeider, bediende, interim, stagiair, tijdelijke arbeidskracht enz. met een ondertekende overeenkomst tussen deze persoon en Orbid.

"Onderaannemer": Personen of bedrijven die geen medewerker zijn bij Orbid maar wel voor Orbid werken en een onderaannemingscontract getekend hebben.

"Derden": Personen die geen medewerker statuut of onder aannemingscontract hebben bij Orbid.

"Gebruiker": Medewerkers of onderaannemers die toegang hebben tot het Orbid IT-netwerk.

"Informatie-item (Information Asset)": elke informatie of informatiesysteem dewelke een bedrijfs-, confidentialiteit- of gevoelswaarde heeft voor Orbid NV, hiertoe behoren ook informatie-items afkomstig van andere partijen die verwerkt worden door Orbid NV.

2. *Het belang van informatieveiligheid*

Als dienstenbedrijf wensen we de informatie die we ontvangen en verwerken optimaal te beschermen met speciale aandacht voor persoonsgegevens.

We engageren ons om conform te zijn met de vereisten, waaronder ook de wettelijke, wat betreft informatiebeveiliging (zoals bijvoorbeeld de GDPR-wetgeving) en vereisen dit ook van onze leveranciers en onderaannemers.

We streven continu naar verbetering, met als doel een veilige informatieomgeving te creëren en ons ISMS te onderhouden en verder uit te bouwen.

In het bijzonder willen we de informatie-items beschermen tegen:

- Verlies: gegevens zijn niet meer beschikbaar
- Lekken: gegevens komen in verkeerde handen terecht
- Fouten: gegevens zijn niet correct, bijvoorbeeld verouderd of onvolledig
- Niet toegankelijk: op het moment van de dienstverlening zijn de gegevens niet toegankelijk
- Onterecht inkijken: ingekeken door personen die hiertoe niet gemachtigd zijn
- Het niet kunnen nagaan wie de gegevens inkeek, wijzigde of verwijderde
- Verwerkingen die niet in lijn liggen met regelgeving, richtlijnen en normen

Orbid NV heeft een Information Security Management System (ISMS) kader opgezet om dit beleid te ondersteunen. Dit omvat processen, procedures en afspraken (policies) dewelke ondersteund

Orbid NV Aaron Business Park Guldensporenpark 20 - Blok C B-9820 Merelbeke T +32 9 272 99 11 | Industriepark E17/1 Zoersenstraat 3 B-9160 Lokeren T +32 9 339 12 47 | Bedrijvencentrum Inzetek Cipalstraat 3 B-3440 Geel T +32 14 57 41 01 | BANK BE47 8410 6282 0180 BTW BE0463 178 208 www.orbid.be

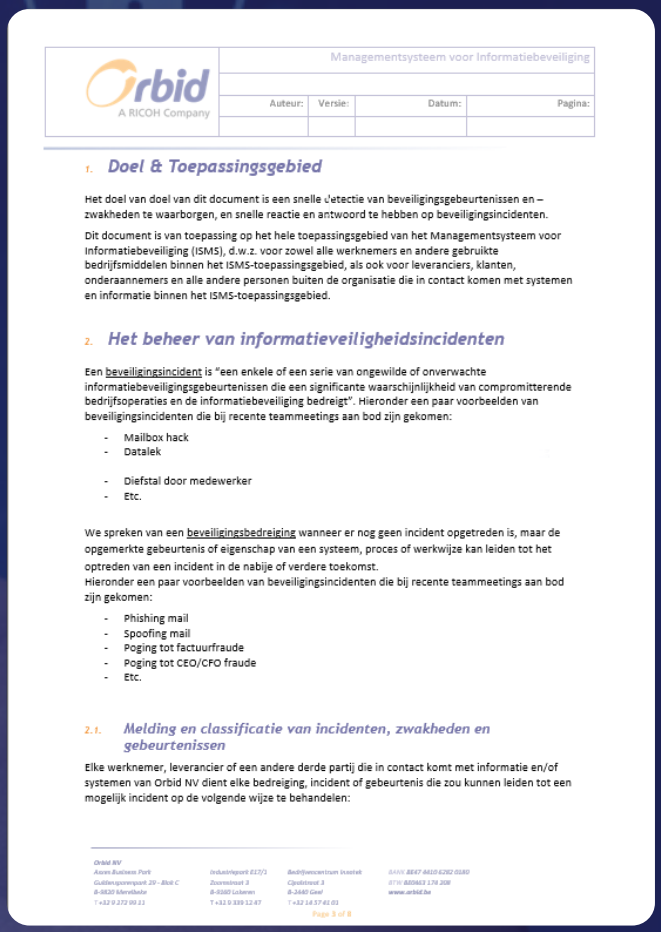
Page 3 of 12

Incidenten- en crisisbeheer

NIS2-maturiteitscheck

In onze template database vindt u ook templates voor een incidenten- en crisisbeleid.

- Basic Incident Respons Plan



Orbid A RICOH Company | Managementsysteem voor Informatiebeveiliging | Auteur: | Versie: | Datum: | Pagina:

1. *Doel & Toepassingsgebied*

Het doel van doel van dit document is een snelle detectie van beveiligingsgebeurtenissen en –zwakheden te waarborgen, en snelle reactie en antwoord te hebben op beveiligingsincidenten.

Dit document is van toepassing op het hele toepassingsgebied van het Managementsysteem voor Informatiebeveiliging (ISMS), d.w.z. voor zowel alle werknemers en andere gebruikte bedrijfsmiddelen binnen het ISMS-toepassingsgebied, als ook voor leveranciers, klanten, onderaannemers en alle andere personen buiten de organisatie die in contact komen met systemen en informatie binnen het ISMS-toepassingsgebied.

2. *Het beheer van informatieveiligheidsincidenten*

Een beveiligingsincident is "een enkele of een serie van ongewilde of onverwachte informatiebeveiligingsgebeurtenissen die een significante waarschijnlijkheid van compromitterende bedrijfsoperaties en de informatiebeveiliging bedreigt". Hieronder een paar voorbeelden van beveiligingsincidenten die bij recente teammeetings aan bod zijn gekomen:

- Mailbox hack
- Datalek
- Diefstal door medewerker
- Etc.

We spreken van een beveiligingsbedreiging wanneer er nog geen incident opgetreden is, maar de opgemerkte gebeurtenis of eigenschap van een systeem, proces of werkwijze kan leiden tot het optreden van een incident in de nabije of verdere toekomst.
Hieronder een paar voorbeelden van beveiligingsincidenten die bij recente teammeetings aan bod zijn gekomen:

- Phishing mail
- Spoofing mail
- Poging tot factuurfraude
- Poging tot CEO/CFO fraude
- Etc.

2.1. *Melding en classificatie van incidenten, zwakheden en gebeurtenissen*

Elke werknemer, leverancier of een andere derde partij die in contact komt met informatie en/of systemen van Orbid NV dient elke bedreiging, incident of gebeurtenis die zou kunnen leiden tot een mogelijk incident op de volgende wijze te behandelen:

Orbid NV Aaron Business Park Guldensporenpark 20 - Blok C B-9820 Merelbeke T +32 9 272 99 11 | Industriepark E17/1 Zoersenstraat 3 B-9160 Lokeren T +32 9 339 12 47 | Bedrijvencentrum Inzetek Cipalstraat 3 B-3440 Geel T +32 14 57 41 01 | BANK BE47 8410 6282 0180 BTW BE0463 178 208 www.orbid.be

Page 3 of 8

Orbid A RICOH Company

Garantie van de bedrijfscontinuïteit

NIS2-maturiteitscheck

Orbid beschikt over verschillende documenttemplates die uw organisatie nodig heeft voor de garantie van de bedrijfscontinuïteit.

- Backup plan
- Business Continuity Plan

Recovery testen via Orbid

Orbid is gespecialiseerd in het uitvoeren van recovery testen van uw kritische data. Zo krijgt u een objectief beeld van hoe uw organisatie ervoor staat.

Immutable Backup as a Service

Via de 'Backup as a Service'-oplossing van Orbid, gebaseerd op de technologie Veeam, zorgt u voor een optimale bescherming van uw bedrijfsgegevens. Onze Backup as a Service is immutable waardoor uw backup ongewijzigd blijft gedurende een aantal dagen.

Backup for Microsoft 365

Microsoft neemt geen backups van uw gegevens. Via de Backup voor Microsoft 365 kan u veilige backups maken van uw data binnen de Microsoft 365 applicaties en opslaan in de cloud of on-premise.

Orbid Private Cloud

Orbid Cloud is een volledig redundante Belgische private cloud in samenwerking met onze partner Datacenter United. We bieden een state-of-the-art platform met internationale reikwijdte, hoge flexibiliteit, snelheid en betrouwbaarheid.

Redundantie

Via oplossingen van partners zoals DataCore (software defined storage) en HPE zorgen we ervoor dat uw omgeving volledig redundant is opgebouwd. Daarnaast kan u ook op firewall niveau zorgen voor redundantie via firewall clustering. Samen met WatchGuard of Fortinet bekijken we de best mogelijke oplossing voor uw organisatie.

Garantie en beveiliging van de continuïteit van uw supply chain

NIS2-begeleiding op maat

Orbid kan u adviseren door een duidelijke procedure op te maken, u te helpen bij het invullen van de vragenlijst en hierna een beoordelingsverslag op te maken.

Beveiliging bij het **verwerven, ontwikkelen en onderhouden** van netwerk- en informatiesystemen

NETWORK SECURITY

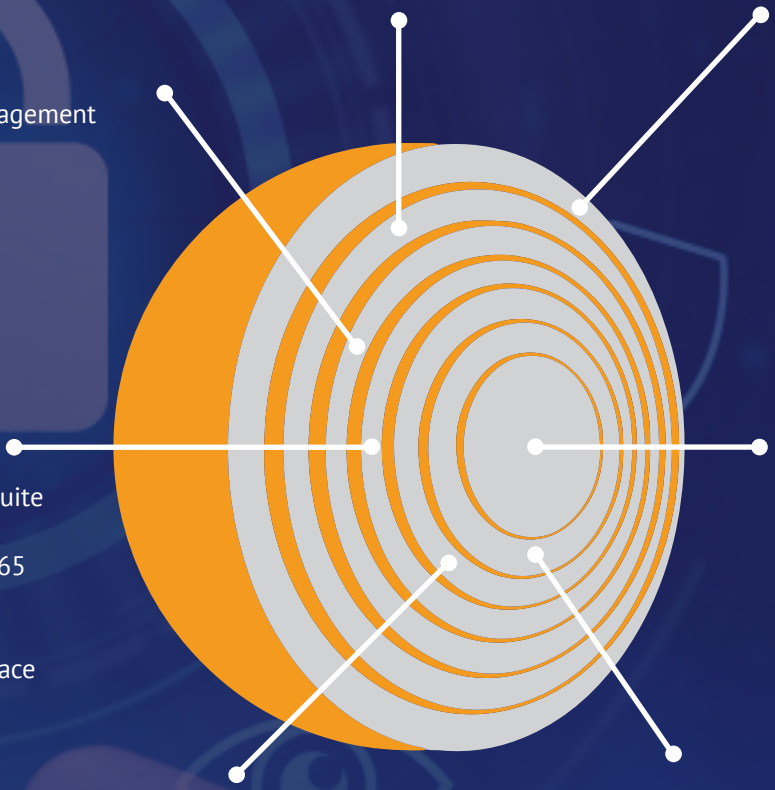
- Aruba Clearpass / Aruba Central
- Wireless security
- VLAN security
- VPN security
- Identity & Access management
- Patch management
- Monitoring

PERIMETER SECURITY

- Firewall (WatchGuard / Fortinet)
- Cloud security via Microsoft 365

THE HUMAN LAYER

- Security awareness



ENDPOINT SECURITY

- Microsoft 365 Defender suite
  - Endpoint
  - Microsoft (Office) 365
  - Servers
  - Microsoft Intune
- Managed Modern Workplace
- Patch management
- Monitoring

MISSION CRITICAL ASSETS

- Vulnerability management
- Log management & log analyse
- ICT security scan

APPLICATION SECURITY

- Security binnen uw (Microsoft 365) apps
- Web application security
- Managed Modern Workplace
- Vulnerability scanning

DATA SECURITY

- Immutable Backup as a Service
- Microsoft 365 Backup
- Encryptie

Een sterk netwerk van security partners

Microsoft · Hewlett Packard Enterprise · HPE aruba networking · WatchGuard · veeam · datacenterunited · DATACORE · ARROW · INGRAM MICRO · DELL Technologies · HOLM SECURITY · CISCO · FORTINET · SentinelOne · CITRIX · vmware · AdminDroid

Orbid A RICOH Company

Beleid en procedures om de **effectiviteit van de maatregelen** te beoordelen

Ethical hacking

Via Orbid kan u een ethical hacker inhuren die grondig door uw systeem gaat om mogelijke lekken op te sporen en om virussen, spyware of cryptolockers te controleren.

Interne & externe audits

De experten van Orbid kunnen uw organisatie ondersteunen bij het houden van interne en externe audits. Onze medewerkers zijn gespecialiseerd in audits zoals voor ISO27001, waarbij we onder andere nagaan wie er kan inloggen op uw systemen, wie MFA heeft ingeschakeld en welke accounts al een bepaald aantal dagen niet meer ingelogd hebben.

Basispraktijken voor **cyberhygiëne**

Security awareness aanpak

Incidenten op basis van menselijke fouten vormen nog steeds de belangrijkste oorzaken van datalekken, downtime en/of reputatieschade voor een bedrijf.

Via onze IT security awareness test kan u uw medewerkers bewustmaken van de technieken die cybercriminelen toepassen. Door de combinatie van phishing simulaties en awarenesstrainingen traint u uw medewerkers om potentiële dreigingen te herkennen en zo het risico op een phishing- of cyberaanval drastisch te verminderen.

Beleid & procedures voor **cryptografie en encryptie**

Beleid rond cryptografie

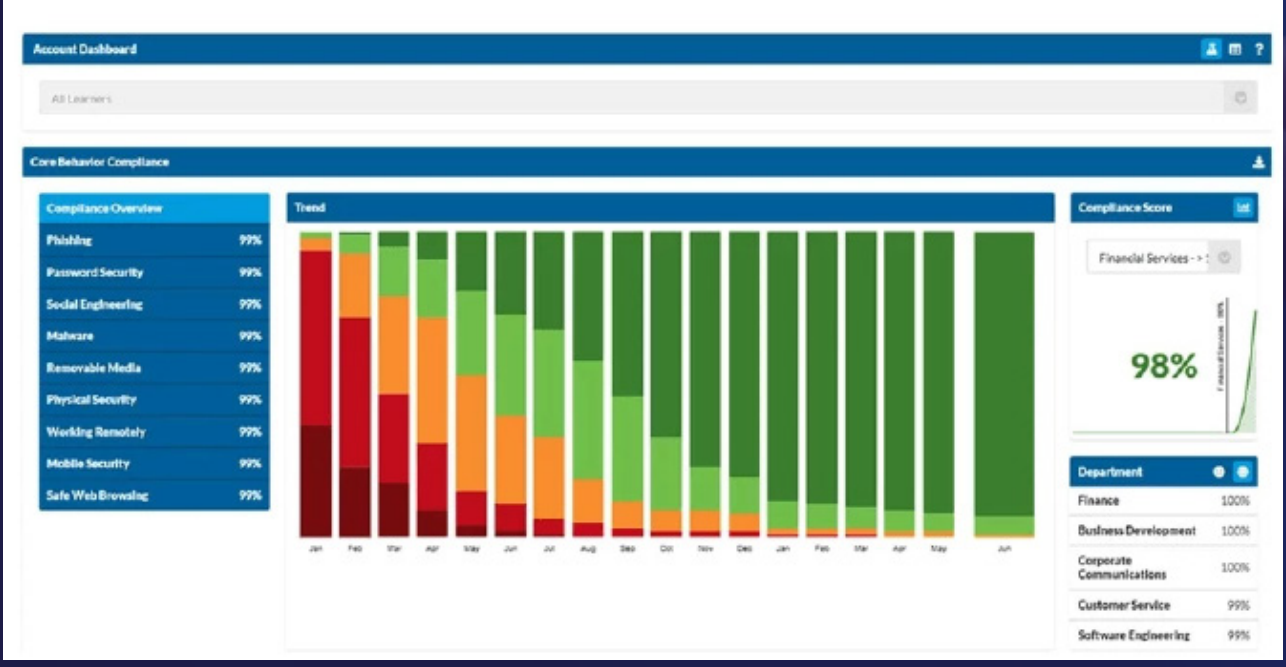
Hebt u nog geen beleid rond cryptografie, dan kan Orbid u ondersteunen bij het opmaken hiervan. Samen met u bepalen we welke maatregelen nodig zijn om uw organisatie zo optimaal mogelijk te ondersteunen.

Bitlocker

Het CCB legt organisaties op om devices te encrypteren via tools zoals Bitlocker. Orbid kan u helpen bij het implementeren van Bitlocker voor al uw toestellen.

HTTPS

Maakt uw organisatie gebruik van één of meerdere websites? Dan moet u als organisatie zeker HTTPS met een officieel certificaat gebruiken om veilig te surfen.



Voorbeeld van een dashboard via onze security awareness aanpak.

Orbid A RICOH Company

Beveiligingsaspecten voor **personeel, toegangsbeleid en beheer van activa**

Creëer security awareness

Zorg voor voldoende cybersecurity awareness bij uw medewerkers via een security awareness training. Neem de security maatregelen ook mee in documenten zoals de onthaalbrochure van nieuwe medewerkers en procedures voor vertrekkende medewerkers.

De Orbid HR-consultants kunnen u hierin ondersteunen.

Toegangsbeleid

Een goed en weldoordacht toegangsbeleid is cruciaal in de beveiliging van uw organisatie. Breng daarom alle toegangen - denk aan toegang tot gebouwen, uw IT-netwerk, servers, maar ook applicaties zoals CRM of uw ERP - in kaart. Alleen zo ziet u welke risico's u loopt en waar de kans het grootst is dat er hackers binnen kunnen sluipen. Maak ook gebruik van een goede Identify & Authentication Management tool (IAM).

Niemand binnen uw organisatie mag voor dagelijkse taken werken met adminrechten. Doe voor Microsoft 365 applicaties een beroep op Priviliged Identity om uw medewerkers 'just in time' en 'just enough' access te verlenen.

Wat betreft de controle op de fysieke toegang, kan u een oplossing integreren in uw receptie. Met een slimme bel, gekoppeld aan een kiosk, kan u elke persoon loggen die uw gebouw betreedt en met wie hij/zij/hun contact heeft gehad. Indien u daar een SmartLocker aan toevoegt, kan u ook de levering en het beheer van pakketten op dezelfde manier beveiligen.

Asset management

Breng naast de toegang ook de verschillende apparaten binnen uw organisaties in kaart. Zorg dat uw apparaten, zowel mobiel als laptops, steeds de nodige beveiligingsupdates krijgen via tools zoals Microsoft Intune.

Daarnaast kan u ook gebruikmaken van Aruba Clearpass om de toegang tot uw netwerk te controleren.

Orbid kan u helpen bij het opzetten van tools zoals Microsoft Intune en Aruba Clearpass.

Gebruik **Multifactor Authenticatie (MFA)** wanneer gepast

MFA-implementatie

MFA is een van de beste veiligheidsmaatregelen om uw organisatie te beschermen waarbij medewerkers naast een wachtwoord ook een extra beveiligingscode moeten ingeven.

Bij Orbid willen we we steeds de juiste balans vinden tussen security en gebruiksvriendelijkheid voor uw medewerkers. Zo vermijden we onnodige frustraties en kunnen uw medewerkers op een veilige manier aan hun data.

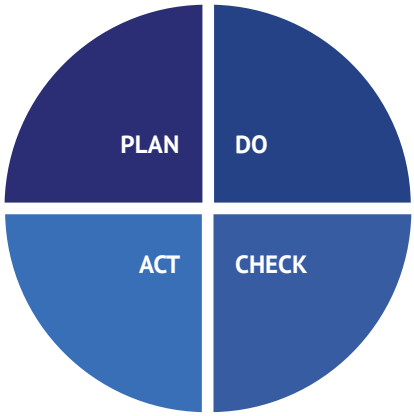
Whitepaper 'Security maatregelen binnen Microsoft 365'

- Til de veiligheid van uw Microsoft 365- apps naar een hoger niveau.
- Behoud de balans tussen security en gebruiksvriendelijkheid.
- Maak gebruik van enkele kickstarts.

Orbid
A RICOH Company

5) Evaluatie en borging

De technieken die cybercriminelen gebruiken, veranderen elke dag. Daarom is het van cruciaal belang dat uw organisatie maatregelen neemt en blijft nemen. **Evalueer regelmatig** of de maatregelen nog steeds up-to-date zijn en evolueer tijdig mee met de voortdurende technologische ontwikkelingen.



Bij Orbid hebben we een **eigen veiligheidsplan** waar we elk jaar gemiddeld 5 à 10 nieuwe maatregelen aan toevoegen op basis van technologische evoluties. Hierbij maken we steeds gebruik van het '**Plan - do - check - act**'-principe.

We zorgen er steeds voor dat we de nodige acties uitvoeren en laten indien nodig een **stuurgroep** per kwartaal de maatregelen opvolgen.

Met de nieuwe NIS2-wetgeving wil de Europese Unie het risico op hacking en de gevolgen ervan verminderen.

Nog enkele extra tips

- **Begin op tijd**. De deadline om in orde te zijn met alle maatregelen is **17 oktober 2024**.
- Voorzie een **budget** voor NIS2.
- Zorg dat je **minimaal in orde** bent met de maatregelen uit **artikel 21**.
- Volg een **risico gebaseerde aanpak** voor uw kritieke business processen.
- **Volg de berichtgeving** rond NIS2 het komende jaar. Enkele regels zijn nog niet volledig vastgelegd en kunnen dus nog wijzigen.

Orbid, uw partner in de transitie naar NIS2

Hebt u ondersteuning nodig in de transitie naar NIS2? Onze experten ondersteunen uw organisatie graag bij het navigeren door de complexiteit van de NIS2-richtlijn. Samen met u bekijken we hoe u op een effectieve en haalbare manier kan voldoen aan de maatregelen.

Expertise in NIS2

Onze experten zijn gespecialiseerd in NIS2. We hebben **diepgaande kennis** van de richtlijn en de impact ervan. Naast **strategisch advies** bieden we ook ondersteuning op het vlak van **technische implementaties**.

Uitgebreide dienstverlening

Onze diensten ondersteunen uw organisatie naadloos in de transitie naar NIS2. Naast onze **IT services** heeft Orbid ook HR-consultants die u kunnen begeleiden bij het opmaken van **policies** voor uw medewerkers.

Focus op evaluatie en borging

Orbid benadrukt het belang van voortdurende evaluatie en borging van security maatregelen. Dit is cruciaal gezien de **continue evolutie van cyberdreigingen** en technologische veranderingen.

Gerpersonaliseerde begeleiding

We volgen steeds een **aanpak op maat**. We starten met een beoordeling van de specifieke behoeften en beveiligingsniveau van een organisatie en komen snel tot een concreet actieplan.

Hulpmiddelen en templates

Orbid heeft **templates en hulpmiddelen** ter beschikking die u kan gebruiken om aan de NIS2-vereisten te voldoen. Zo laat u het proces van naleving efficiënter en gestroomlijnder verlopen.

ISO27001 gecertificeerd

Orbid is ISO27001 gecertificeerd waarmee we bewijzen dat we voldoen aan de hoge internationale norm voor **informatiebeveiliging** en dus ook meteen **NIS2-compliant** zijn.

Maak kennis met onze 'Managed Modern Workplace'-oplossing

In de moderne werkplek zijn devices, tools en medewerkers continu verbonden. Deze toegenomen mobiliteit - op en naast de werkvloer - brengt uitdagingen met zich mee: een **goede balans** vinden tussen security en gebruiksvriendelijkheid is niet evident en het onderhouden van de moderne werkplek vraagt veel tijd aan uw IT-afdeling. NIS2 zal deze uitdagingen alleen maar versterken.

Via de 'Managed Modern Workplace'-oplossing van Orbid kan u het beheer van uw moderne werkplek **geheel of gedeeltelijk uitbesteden** aan de experten van Orbid tegen een **vast en voorspelbaar bedrag** per maand. Zo hebt u steeds toegang tot de nieuwste en veiligste technologieën en kan uw IT-afdeling tijd vrijmaken om zich te **focussen op hun core activiteiten**.

Microsoft Solutions Partner
Modern Work

Orbid is trots erkend te zijn als **Solutions Partner Modern Work**. Op basis van criteria zoals prestaties, skills en realisaties bij onze klanten, tonen we aan dat we over een brede capaciteit beschikken om organisaties te ondersteunen bij het verhogen van hun productiviteit en de switch te maken naar de moderne werkplek. Meer info leest u op onze website.

Orbid
A RICOH Company

Wenst u meer informatie?

Contacteer gerust onze experten, wij helpen u graag verder.

Axxess Business Park (HQ)
Guldensporenpark 29 - Blok C
B-9820 Merelbeke
T +32 9 272 99 11

Industriepark E17/1
Zoomstraat 3
B-9160 Lokeren
T +32 9 339 12 47

Orbid Geel
Liesdonk 5
B-2440 Geel
T +32 14 57 41 01

info@orbid.be • www.orbid.be

Orbid
A RICOH Company