Ministerie van Economische Zaken
en Klimaat

Wet Beveiliging Netwerk- en Informatiesystemen *(Wbni)* voor **Digitale dienstverleners**

De Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) zal binnenkort in werking treden. De wet is van toepassing op organisaties die vitaal zijn én op digitale dienstverleners. Dit document richt zich uitsluitend op de laatste categorie, de digitale dienstverleners.

Dit document bestaat uit de volgende onderdelen:

1. Inleiding

Om Nederland digitaal veiliger te maken treedt binnenkort de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) in werking. In de wet staan maatregelen om de digitale weerbaarheid te vergroten. Organisaties in vitale sectoren en digitale dienstverleners krijgen een meldplicht van incidenten op netwerk- en informatiesystemen en een zorgplicht (het treffen van beveiligingsmaatregelen ten aanzien van hun netwerk vitale aanbieders- en informatiesystemen).

De Wet Beveiliging Netwerk- & Informatiesystemen (Wbni)

De Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) is de Nederlandse vertaalslag van de Europese Netwerk- en Informatiebeveiligingsrichtlijn (de NIB-Richtlijn).[1] Deze richtlijn is medio 2016 gepubliceerd en verplicht alle EU-lidstaten om deze richtlijn om te zetten in nationale wetgeving; dat is in Nederland de Wbni geworden.

De Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) geldt voor vitale aanbieders uit ondermeer de energie-, de financiële- en vervoerssector. Vitale diensten zijn van essentieel belang voor het goed functioneren van de Nederlandse samenleving en economie; als de ict-systemen van deze diensten worden gecompromitteerd of uitvallen, dan kan dat zeer grote gevolgen hebben voor een betrouwbare dienstverlening aan burgers en bedrijven.

Naast de vitale aanbieders geldt de Wbni ook voor digitale dienstverleners. Hoewel zij niet als vitaal worden beschouwd, zijn ze belangrijk: veel burgers/consumenten en bedrijven maken gebruik van of zijn afhankelijk van deze dienstverlening. Daarom zijn ze in de NIB-richtlijn opgenomen. De netwerk- en informatiesystemen die nodig zijn om vitale diensten of digitale diensten aan te kunnen bieden moeten betrouwbaar zijn en dienen dus goed beveiligd te zijn. De zorgplicht uit de Wbni moet leiden tot het treffen van de goede beveiligingsmaatregelen door vitale aanbieders en digitaledienstverleners. Incidenten die zich ondanks die zorgplicht toch voordoen en die deze beveiliging in gevaar brengen moeten bij de overheid worden gemeld (de meldplicht uit de Wbni).

In dit document gaat het alleen over de gevolgen van de Wbni voor de digitale dienstverleners. Digitale dienstverleners zijn aanbieders van clouddiensten, online zoekmachines en online marktplaatsen. Ze worden hier ook DSP's genoemd, oftewel Digital Service Providers. Algemene informatie over de wet en voor aanbieders van vitale diensten is terug te vinden op de website van het Nationaal Cyber Security Centrum https://www.ncsc.nl/actueel/dossiers/wetgeving-cybersecurity.html

Mochten er nieuwe ontwikkelingen zijn of mocht uit vragen en feedback vanuit ondernemingen blijken dat in bepaalde informatiebehoefte nog niet is voorzien, dan zal voor aanvullende informatie worden gezorgd.

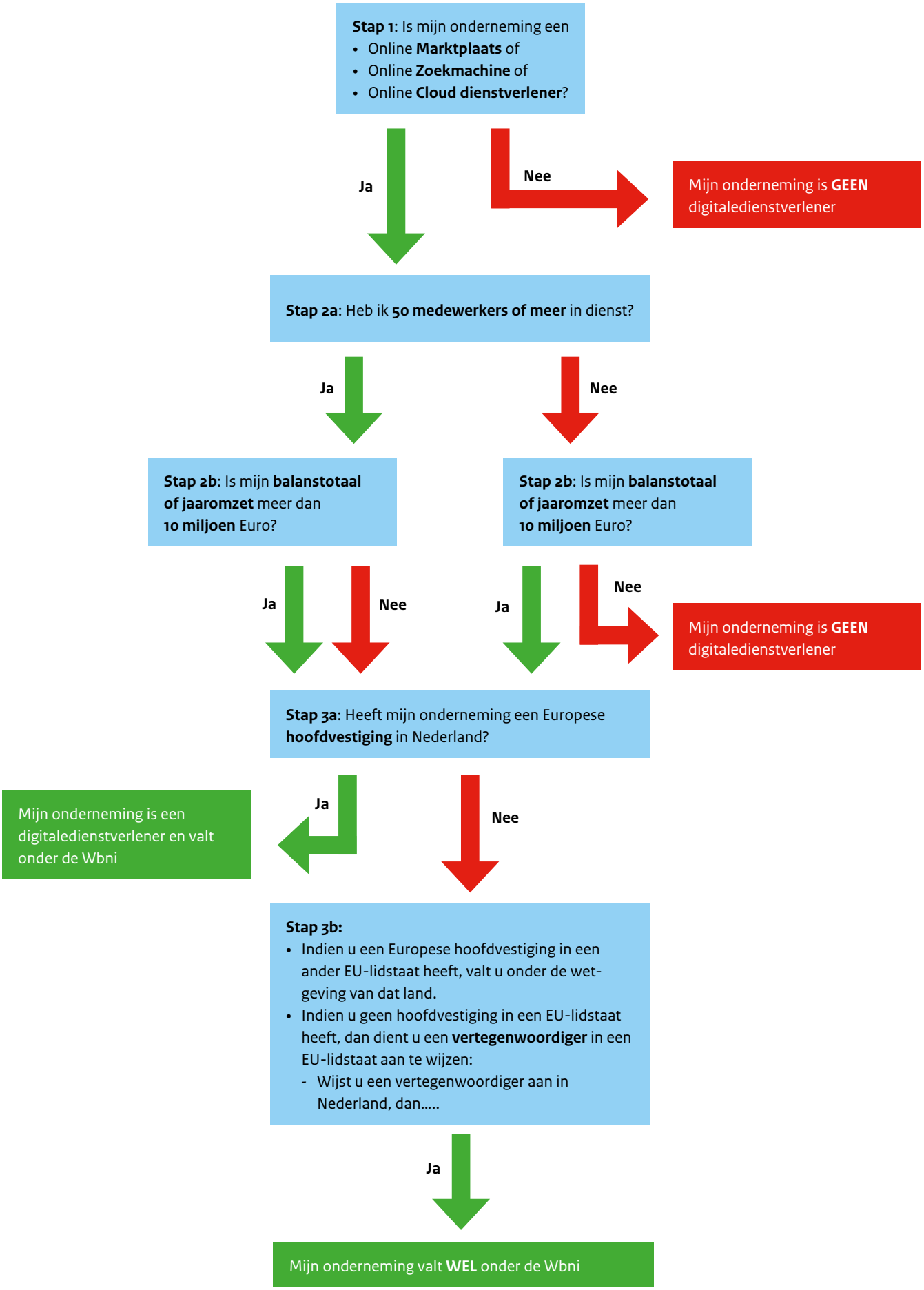
Voor een goede leesbaarheid zijn niet altijd de letterlijke wetsteksten in dit document opgenomen; er wordt verwezen naar de relevante artikelen zodat de wetsteksten altijd kunnen worden opgezocht.

[1] Richtlijn (EU) 2016/1148 van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

2. Wie is een digitale dienstverlener?

In de Europese richtlijn Netwerk- en Informatiebeveiliging (NIB) is bepaald wie een digitale dienstverlener is: niet elke partij die een digitale dienst aanbiedt, valt automatisch onder de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni). Zo zijn er allerlei digitale diensten die niet onder de regelgeving vallen, zoals social media of webshops. En alleen digitale dienstverleners vanaf een bepaalde omvang kunnen onder de Wbni vallen. Daarom wordt hier eerst uitgelegd wat onder een digitale dienstverlener wordt verstaan. En mocht u een digitale dienstverlener zijn, dan zal moeten worden bepaald onder welke de jurisdictie (rechtsgebied) uw onderneming komt te vallen. Dit is relevant om te bepalen of uw onderneming onder de Nederlandse wet (Wbni) komt te vallen of onder de wetgeving van een andere EU-lidstaat. Deze jurisdictievraag is vooral van belang voor ondernemingen die hun diensten in meerdere EU-lidstaten aanbieden.

Aan de hand van onderstaand schema kunt u bepalen of uw onderneming een digitale dienstverlener is zoals bedoeld in de Wbni (stappen 1, 2a en 2b). Mocht dat het geval zijn, dan kunt u schema verder doorlopen om te bepalen welk rechtsgebied van toepassing is (stappen 3a en 3b).


Stap 1: Is mijn onderneming een
• Online **Marktplaats** of
• Online **Zoekmachine** of
• Online **Cloud dienstverlener**?
Ja
Nee
Mijn onderneming is **GEEN** digitaledienstverlener
Stap 2a: Heb ik **50 medewerkers of meer** in dienst?
Ja
Nee
Stap 2b: Is mijn **balanstotaal of jaaromzet** meer dan **10 miljoen** Euro?
Stap 2b: Is mijn **balanstotaal of jaaromzet** meer dan **10 miljoen** Euro?
Ja
Nee
Ja
Nee
Mijn onderneming is **GEEN** digitaledienstverlener
Stap 3a: Heeft mijn onderneming een Europese **hoofdvestiging** in Nederland?
Mijn onderneming is een digitaledienstverlener en valt onder de Wbni
Ja
Nee
Stap 3b:
• Indien u een Europese hoofdvestiging in een ander EU-lidstaat heeft, valt u onder de wet-geving van dat land.
• Indien u geen hoofdvestiging in een EU-lidstaat heeft, dan dient u een **vertegenwoordiger** in een EU-lidstaat aan te wijzen:
- Wijst u een vertegenwoordiger aan in Nederland, dan.....
Ja
Mijn onderneming valt **WEL** onder de Wbni

Toelichting op Schema 1

Stap 1: Digitale dienst

Stap 1: Om te bepalen of u één of meerdere digitale diensten aanbiedt zoals bedoeld in de wet, moet worden gekeken of uw dienst(en) voldoet aan de definitie van "Online marktplaats" of "Clouddiensten" of "Online zoekmachines". Deze definities worden hieronder nader toegelicht.

Online marktplaats[2]
Een online marktplaats is een website waarop ondernemers of consumenten verkoop- of dienstenovereenkomsten kunnen sluiten met (andere) ondernemers.

Uw organisatie valt hieronder als:

- u als platform of website verkopen faciliteert tussen koper en verkoper. Hierbij wordt gebruik gemaakt van informaticadiensten van het platform. Denk bijvoorbeeld aan het verwerken van de betalingen door het platform; het platform faciliteert op deze manier de totstandkoming van de overeenkomst.
- de aankoop wordt gesloten op de website van de marktplaats of op de website van de (verkopende) ondernemer.
- er sprake is van drie partijen: de koper, verkoper en de marktplaats.
  - Uitzondering: het gaat dus niet om webshops en vergelijkingssites zijn uitgesloten.

Een onlinemarktplaats kan zich in elke sector voordoen, bijvoorbeeld retail, reizen, verkoop van elektronische inhoud (appstores) en handelsplatforms voor olie of energie. Online marktplaatsen kunnen zowel de Business to Business (B-to-B)- als Business-to-Consumer (B-to-C) markt bedienen.

Op bladzijde 8 staan enkele concrete voorbeelden van online marktplaats beschreven.

Online zoekmachine[3]
Een online zoekmachine is een digitale dienst die het gebruikers mogelijk maakt zoekacties uit te voeren op in beginsel alle websites.

Als u op uw website een zoekfunctie aanbiedt om uitsluitend binnen uw website naar informatie te zoeken, is uw organisatie geen "online zoekmachine" zoals hier is bedoeld.

Clouddienstverlener[4]
Clouddienstverleners leveren een digitale dienst die toegang mogelijk maakt tot een schaalbare en elastische pool van deelbare computercapaciteit. Clouddienstverleners leveren diensten die overal en altijd toegankelijk zijn.

De meeste clouddiensten kunnen in drie hoofdcategorieën worden onderverdeeld: Software as a Service (Saas), Platform as a Service (PaaS) en Infrastructure as a Service (IaaS). Deze vallen qua kenmerken onder de definitie van clouddiensten zoals hierboven is omschreven.

Software as a Service (SaaS): een "online" applicatie die vanuit een webbrowser, plaats en tijdonafhankelijk, kan worden bediend. Bijvoorbeeld een financieel pakket, online office, etc.

Platform as a Service (PaaS): een "online, ingericht" platform waarop de gebruiker of klant eigen software diensten kan draaien of platformen die specifieke functionaliteit aanbieden. Bijvoorbeeld een "virtuele PC met een besturingssysteem", een authenticatieplatform of een opslag.

Infrastructure as a Service (IaaS): de virtuele hardware laag waarin de gebruiker of klant eigen netwerken, opslag, servers en werkstations kan aanmaken en beheren. Bijvoorbeeld virtuele werkplekken, gegevensopslag, netwerkapparatuur. Hierop kan de gebruiker of klant eigen besturingssystemen en configuraties installeren.

Uitzondering :
Privé cloud dienstverlening, bijvoorbeeld clouddiensten die binnen één organisatie alleen worden gebruikt door die organisatie, vallen niet onder de definitie van clouddienstverlener.

Stap 2a en Stap 2b: Omvangcriteria aantal medewerkers en balanstotaal/jaaromzet

De Wbni geldt alleen voor (middel)grote ondernemingen en niet voor micro- en kleine ondernemingen. Om te bepalen of een onderneming micro of klein is wordt gekeken naar het aantal medewerkers en balanstotaal/jaaromzet. U bent een digitale dienstverlener indien u 50 medewerkers of meer in dienst heeft en/of de balanstotaal of jaaromzet meer dan 10 miljoen Euro per jaar bedraagt. Hieronder wordt op deze criteria nader ingegaan.

Aantal medewerkers
Indien het aantal medewerkers 50 of meer is, dan bent u geen micro- en kleine onderneming. Hoe moet het aantal medewerkers worden berekend?

- De gegevens voor de berekening van het aantal werkzame personen hebben betrekking op het laatste afgesloten boekjaar.
- Het aantal werkzame personen komt overeen met het aantal arbeidsjaareenheden (AJE); dat wil zeggen het aantal personen dat het gehele desbetreffende jaar voltijds in de betrokken onderneming of voor rekening van deze onderneming heeft gewerkt. Het werk van personen die niet het gehele jaar hebben gewerkt, deeltijdwerk ongeacht de duur ervan, worden in breuken van AJE uitgedrukt.

[2] Artikel 4, 17e lid en overweging nr. 15 NIB-Richtlijn (EU) 2016/1148.
[3] Artikel 4, 18e lid en overweging nr. 16 NIB-Richtlijn (EU) 2016/1148.
[4] Artikel 4, 19e lid en overweging nr. 17 NIB-Richtlijn (EU) 2016/1148.

- Het aantal werkzame personen bestaat uit:
  a. de loontrekkenden;
  b. de personen die voor deze onderneming werken, er een ondergeschikte verhouding mee hebben en voor het nationale recht met loontrekkenden gelijkgesteld zijn;
  c. de eigenaren-bedrijfsleiders;
  d. de vennoten die geregeld een activiteit in de onderneming uitoefenen en van de onderneming financiële voordelen genieten.
- Leerlingen en studenten die een beroepsopleiding volgen en een leer- of beroepsopleidingsovereenkomst hebben, worden *niet* meegeteld in het aantal werkzame personen. De duur van zwangerschaps- en ouderschapsverlof wordt niet meegerekend.

Balanstotaal of jaaromzet
Indien uw balanstotaal of jaaromzet meer dan 10 miljoen Euro bedraagt, dan valt u onder de wet. Hoe moet dat worden berekend?
- De gegevens voor de berekening van de financiële bedragen hebben betrekking op het laatste afgesloten boekjaar. Zij worden vanaf de datum van afsluiting van de rekeningen in aanmerking genomen.
- Het bedrag van de omzet wordt berekend exclusief belasting over de toegevoegde waarde (BTW) en andere indirecte rechten of heffingen.
- In het geval van recent opgerichte ondernemingen waarvan de eerste jaarrekening nog niet is goedgekeurd, kan een schatting van de gegevens worden gemaakt.

Nog een aandachtspunt bij de omvangcriteria:
- Indien uw onderneming banden heeft met andere ondernemingen, bijvoorbeeld door middel van een holdingstructuur, dan is de vraag aan de orde in hoeverre deze andere ondernemingen moeten worden meegerekend bij het bepalen van het "aantal medewerkers" of de "balanstotaal of omzet". De mate van verbondenheid met deze andere ondernemingen bepaalt of het als één geheel danwel als meerdere zelfstandige ondernemingen moet worden beschouwd.

Meer informatie over deze verbondenheid en over de hierboven genoemde omvangscriteria kunt u dit terugvinden in:
- "Aanbeveling van de Europese Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (2003/361/EG)": hieronder staat de link:
- https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32003H0361
- de "Gebruikersgids bij de definitie van kmo's"[5], een publicatie van de Europese Commissie[6]. Deze gids bevat een uitgebreide toelichting en een aantal voorbeelden om de verbondenheid van ondernemingen te kunnen bepalen. Hieronder de link: https://www.rvo.nl/file/de-nieuwe-definitie-van-kmo of https://publications.europa.eu/nl/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1/language-nl (in meerdere talen beschikbaar)

Stap 3: Hoofdvestiging in Nederland / vertegenwoordiger aanwijzen

- Indien u een digitale dienst aanbiedt en aan één van de hierboven genoemde twee omvangscriteria voldoet, dan bent u een digitale dienstverlener. Vervolgens dient te worden bepaald of u onder de Nederlandse wet (jurisdictie) valt of onder de NIB-wetgeving van een ander EU-lidstaat. Dat is onder andere van belang om te bepalen in welk land u een incidentmelding moet doen of met welke toezichthouder u te maken krijgt.
- Om te bepalen of de Nederlandse wet voor u van toepassing is, moet hiervoor de volgende stappen worden doorlopen:
  1. Eerst moet worden gekeken of u een hoofdvestiging heeft in een lidstaat van de Europese Unie. Heeft u uw Europese hoofdvestiging in Nederland, dan valt u onder de Wbni. Indien uw Europese hoofdvestiging in een ander EU-lidstaat is gevestigd, dan valt u onder de wetgeving van dat land.
  2. Indien u geen hoofdvestiging in een EU-lidstaat heeft, bijvoorbeeld omdat uw hoofdvestiging in een Europees land is gevestigd dat geen deel uitmaakt van de Europese Unie, dan dient u een vertegenwoordiger in een EU-lidstaat aan te wijzen.
     - Kiest u er voor om een vertegenwoordiger in Nederland aan te wijzen, dan valt u onder de Wbni.
     - Kiest u er voor om een vertegenwoordiger in een andere EU-lidstaat aan te wijzen, dan valt u onder de wetgeving van dat land.

[5] De gids gaat in op kleine, middelgrote en micro-ondernemingen (kmo's). Dat betekent dat de gids op sommige plaatsen de criteria voor middelgrote ondernemingen weergeeft. De NIB-richtlijn en Wbni gelden niet voor micro- en kleine ondernemingen maar wel voor (middel)grote ondernemingen. Pagina 11 vermeldt de drempels die voor de verschillende categorieën gelden.
[6] "Gebruikersgids bij de definitie van kmo's", Europese Commissie, Ref. Ares(2016)956541 – 24/02/2016.

Casuïstiek Online marktplaats

Casus online marktplaats (Business to Consumer)

- Een supermarkt biedt consumenten de mogelijkheid om ook online boodschappen te kunnen doen. Deze supermarkt verkoopt producten van het eigen huismerk maar ook van talloze andere merken, maar daarmee is een supermarkt nog geen online marktplaats zoals in de Wet Beveiliging Netwerk- en Informatiesystemen wordt bedoeld. Immers, de consument sluit de koop niet met die andere merken maar met de supermarkt. Hier is sprake van een webshop.
- Stel dat de supermarkt besluit om ook producten namens andere verkopers of leveranciers te verkopen: de supermarkt gaat via haar webshop streekproducten aanbieden; die producten maken geen deel uit van de gebruikelijke voorraad van de supermarkt, zoals dat bij de hierboven genoemde merken wel is.
- De supermarkt geeft op haar website aan dat de streekproducten door lokale ondernemers worden aangeboden en dat de consument uiteindelijk de koop sluit met de lokale ondernemer. De supermarkt voert een aantal activiteiten namens de lokale ondernemers uit, bijvoorbeeld het verwerken van de betalingstransactie.
- De supermarkt neemt zodoende verschillende activiteiten van de lokale ondernemer uit handen en de aanbieder van de streekproducten krijgt haar deel van de betaling. Het kan zijn dat de lokale ondernemer zelf de producten bezorgt maar dat kan ook de supermarkt zijn. Alleen voor het verkopen van de streekproducten is de supermarkt een online marktplaats, niet voor de overige activiteiten.
- Overigens hoeft het niet alleen om de verkoop van producten te gaan. Mocht de supermarkt dezelfde constructie bedenken maar dan voor het aanbieden van tuinonderhoud door een hovenier dan is er ook sprake van een online marktplaats, omdat er een dienst (tuinonderhoud) wordt aangeboden.

Waarom is de supermarkt door de verkoop van streekproducten een online marktplaats?

- Er is sprake van 3 partijen: de koper (consument), de online marktplaats (supermarkt) en de verkoper (aanbieder van streekproducten);
- De koop wordt tussen een klant en een derde partij gesloten (aanbieder van de streekproducten);
- De koop wordt gesloten op de website van de online marktplaats (supermarkt); het had eventueel ook op de website van de lokale ondernemer kunnen zijn;
- Er wordt gebruik gemaakt van informaticadiensten van de onlinemarktplaats (de supermarkt verwerkt de betalingstransactie met gebruikmaking van ict);

Casus online marktplaats (Business to Business)

- Een onlinemarktplaats brengt via vraag naar en aanbod van werk voor ZZP'ers bij elkaar. Een ZZP'er zoekt via het online platform een opdracht en potentiële opdrachtgevers bieden via het online platform opdrachten voor ZZP'ers aan.
- Indien de ZZP'er een geschikte opdracht vindt bij een opdrachtgever, dan wordt na bemiddeling via het online platform een overeenkomst gesloten tussen de zelfstandige en de opdrachtgever.

Waarom is hier sprake van een onlinemarktplaats?

- Er is sprake van drie partijen: de ZZP'er (business), de online marktplaats (bemiddeling) en de andere business (de opdrachtgever).
- De overeenkomst wordt tussen ZZPer en de derde partij gesloten, het bedrijf dat een ZZP kracht zoekt.
- De overeenkomst komt tot stand via de website van de bemiddelaar.
- Er worden ICT middelen ingezet om vraag en aanbod aan elkaar te koppelen.

3. Wat staat er in de Wbni?

Organisaties die vallen onder de Wet beveiliging netwerk- & informatiesystemen (Wbni) hebben een meldplicht- en zorgplicht:

a. De *meldplicht* houdt in dat incidenten onverwijld moeten worden gemeld bij de toezichthouder Agentschap Telecom en bij het CSIRT (Computer Security Incident Response Team) voor digitale diensten. Beide organisaties zijn onderdeel van het Ministerie van Economische Zaken en Klimaat (EZK).
b. De *zorgplicht* houdt in dat een digitale dienstverlener passende organisatorische en technische maatregelen moeten nemen om risico's voor de beveiliging van hun ict-systemen te beheersen en de gevolgen van incidenten te verkleinen. Hiermee kunnen incidenten worden voorkomen en het effect worden geminimaliseerd.

Ad. A) De meldplicht van incidenten

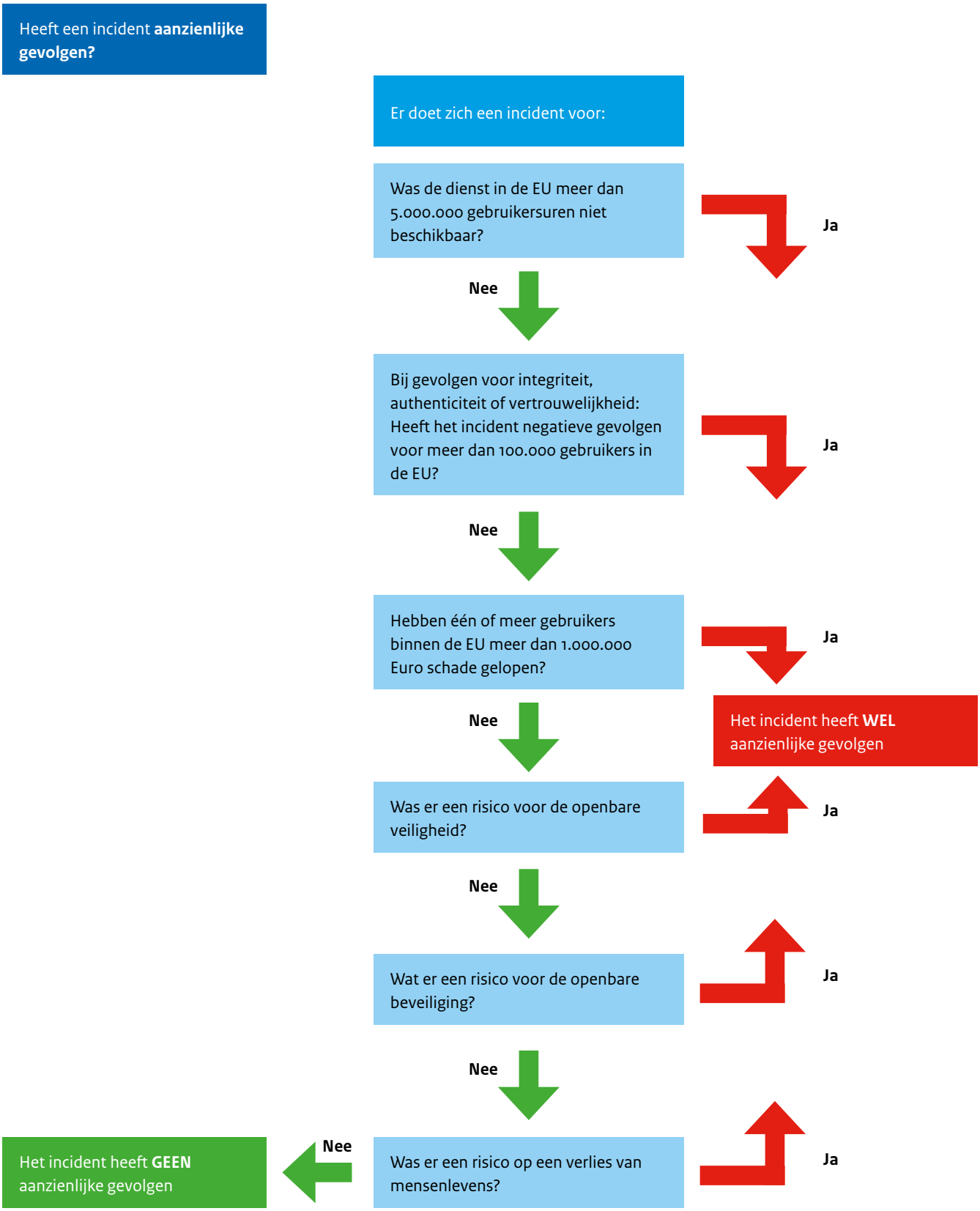
Incidenten moeten worden gemeld. Maar wat wordt in deze wet onder een incident verstaan?

Een incident

Een incident is "elke gebeurtenis met een schadelijk effect op de beveiliging van netwerk- en informatiesystemen"[7].
Bij de beveiliging van netwerk- & informatiesystemen gaat het om beschikbaarheid, integriteit, vertrouwelijkheid, en authenticiteit (biva) van netwerk- en informatiesystemen. Bij de beveiliging

Moet elk incident worden gemeld? Nee, niet elk incident hoeft te worden gemeld. U moet vaststellen of het incident *aanzienlijke* gevolgen voor uw dienstverlening heeft, want alleen die incidenten moeten worden gemeld. Het gaat hierbij ondermeer om het aantal gebruikers dat door de verstoring van de dienst wordt getroffen of de gevolgen van een incident voor economische en maatschappelijke activiteiten. In Europese regelgeving is dit nader uitgewerkt[8].
Er gelden drempelwaarden om te bepalen of een incident moet worden gemeld. Die staan in onderstaand stroomschema weergegeven.

[7] Artikel 4, 7e lid van Richtlijn (EU) 2016/1148 van 6 juli houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de EU.
[8] Artikel 4, uitvoeringsverordening (EU) 2018/151 van 30 januari 2018 (deze verordening heeft uitsluitend betrekking op digitale dienstverleners).


Heeft een incident **aanzienlijke gevolgen?**
Er doet zich een incident voor:
Was de dienst in de EU meer dan 5.000.000 gebruikersuren niet beschikbaar?
Ja
Nee
Bij gevolgen voor integriteit, authenticiteit of vertrouwelijkheid: Heeft het incident negatieve gevolgen voor meer dan 100.000 gebruikers in de EU?
Ja
Nee
Hebben één of meer gebruikers binnen de EU meer dan 1.000.000 Euro schade gelopen?
Ja
Nee
Het incident heeft **WEL** aanzienlijke gevolgen
Was er een risico voor de openbare veiligheid?
Ja
Nee
Wat er een risico voor de openbare beveiliging?
Ja
Nee
Was er een risico op een verlies van mensenlevens?
Ja
Nee
Het incident heeft **GEEN** aanzienlijke gevolgen

Toelichting op het schema

Met betrekking tot "niet beschikbaar" zijn: Onder "gebruikers-uren" wordt verstaan:

het aantal gebruikers in de Europese Unie X het aantal uren dat de digitale dienst niet beschikbaar is

Bijvoorbeeld als de digitale dienst voor 2 miljoen gebruikers niet meer beschikbaar is, moet de verstoring minimaal 2,5 uur duren om de drempelwaarde van de meldplicht te halen.

De incidenten met risico's voor de openbare veiligheid en – beveiliging en risico's voor verlies van mensenlevens die in het schema worden genoemd moeten worden gemeld omdat hier sprake is van een incidenten met economische en/of maatschappelijke impact. Dan gaat het dus over het doel waarvoor een digitale dienst wordt ingezet. Denk bijvoorbeeld aan clouddiensten die voor surveillance-activiteiten door politie of marechaussee wordt ingezet of clouddiensten in de medische sector.

Waar moet een incident worden gemeld?

Een incident onverwijld melden bij Agentschap Telecom en bij het CSIRT voor digitale dienstverleners.

- Agentschap Telecom (AT) is de toezichthouder voor deze digitale dienstverleners. In de Wbni heet dat de "bevoegde autoriteit". De taak van Agentschap Telecom is om toe te zien op de naleving van de wet. Dit kan via www.agentschaptelecom.nl/wbni.
- Het CSIRT voor digitale diensten heeft een andere taak; het CSIRT kan uw onderneming advies geven als er zich een incident heeft voorgedaan. Dit richt zich vooral op incident-response om zodoende de economische en eventueel maatschappelijke schade van een incident te beperken. Het kan eventueel ook andere digitale dienstverleners waarschuwen als er zich een bepaald type incident voordoet. Het is niet de taak van het CSIRT om te controleren of een organisatie zich aan de wet heeft gehouden.
- Agentschap Telecom en het CSIRT voor digitale diensten zijn allebei onderdeel van het Ministerie van Economische Zaken en Klimaat.

Ad. B. Zorgplicht – het treffen van beveiligingsmaatregelen

Digitale dienstverleners zijn verplicht om *passende en evenredige organisatorische en technische* maatregelen te treffen om de *risico's* voor de beveiliging van hun netwerk- en informatiesystemen te beheersen. De maatregelen zorgen, gezien de stand van de techniek, voor een niveau van beveiliging dat is afgestemd op de risico's die zich voordoen.[9]

Bij de *beveiliging van netwerk- en informatiesystemen*[10] gaat het erom dat de netwerk- en informatiesystemen bestand te zijn tegen acties die de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit (biva) van de opgeslagen, verzonden of verwerkte gegevens van die netwerk- en informatiesystemen in gevaar brengen. Dat geldt ook voor de diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn.

De beveiligingsmaatregelen[11] hebben betrekking op:
1. De beveiliging van systemen en voorzieningen;
2. Behandeling van incidenten;
3. Beheer van de bedrijfscontinuïteit;
4. Toezicht (monitoring), controle (auditing) en testen;
5. Inachtneming van de internationale normen.

De vijf hierboven genoemde beveiligingsmaatregelen zijn nader uitgewerkt in artikel 2 van de uitvoeringsverordening (EU) 2018/151 van de Europese Commissie van 30 januari 2018.
Zie bijgaande link: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32018R0151.

De beveiligingsmaatregelen gaan vooral in op WAT er moet worden geregeld en niet zozeer HOE dat zou moeten gebeuren. Zo staat bijvoorbeeld in deze verordening dat met betrekking tot de beveiliging van systemen en voorzieningen maatregelen moeten worden getroffen met betrekking tot de toegangscontroles voor de netwerk- en informatiesystemen. Of met betrekking tot behandeling van incidenten dat detectieprocedures moeten worden gehandhaafd en getest om ervoor te zorgen dat afwijkende gebeurtenissen op tijd worden opgemerkt. Hoe een digitale dienstverlener dit allemaal regelt, is niet voorgeschreven.

Toezichthouder Agentschap Telecom

De toezichthouder heeft de bevoegdheid om bij u informatie op te vragen om te kunnen beoordelen of de beveiliging van de netwerk- & informatiesystemen op orde is. Dat betekent ook dat u over documentatie moet beschikken zodat de toezichthouder kan nagaan of uw onderneming zich aan de beveiligingseisen houdt. Agentschap Telecom komt in beeld na een incident of bij een vermoeden van een overtreding van de wet.

Als toezichthouder heeft Agentschap Telecom een aantal middelen tot haar beschikking om te handhaven; met name:
- Er kan een bindende aanwijzing worden gegeven die het de digitale dienstverlener verplicht om binnen een redelijke termijn bepaalde maatregelen te treffen;
- Er kan een last onder bestuursdwang of een bestuurlijke boete worden opgelegd.

[9] Artikel 7, Eerste Kamer, Regels ter implementatie van Richtlijn (EU) 2016/1148 Wet beveiliging netwerk- en informatiesystemen (Wbni), nr. 34883 A – gewijzigd voorstel van wet, 29 mei 2018.
[10] Artikel 4, tweede lid NIB-Richtlijn (EU) 2016/1148
[11] Artikel 2 Beveiligingselementen, Uitvoeringsverordening (EU) 2018/151 van 30 januari 2018

4. Veel gestelde vragen

Vraag 1

Hoe weet ik of mijn onderneming aan deze wet moet voldoen?
De wet geldt voor digitale dienstverleners. Het gaat om aanbieders van clouddiensten, zoekmachines en onlinemarktplaatsen en geldt alleen voor organisaties vanaf een bepaalde omvang (in omzet/balanstotaal of aantal medewerkers); micro- en kleine ondernemingen zijn uitgesloten. Er zijn dus criteria om te bepalen of een organisatie een digitale dienstverlener is zoals in de wet is bedoeld.

Vraag 2

Wat moet ik doen als mijn onderneming nu niet aan de criteria voldoet om onder de wet te vallen, maar mogelijk volgend jaar wel? Moet ik dan plotseling aan alle verplichtingen voldoen?
Het kan zijn dat op dit moment uw onderneming niet onder de wet valt, bijvoorbeeld omdat uw onderneming klein is. Echter, uw onderneming kan in de toekomst wel onder de wet vallen, bijvoorbeeld omdat uw onderneming is gegroeid, aan de omvangscriteria voldoet en dus een (middel)grote onderneming is geworden. Om enige stabiliteit en zekerheid aan ondernemingen te bieden, dienen ondernemingen twee opeenvolgende boekjaren dezelfde status te hebben – wel of geen micro/kleine onderneming – om van status te veranderen. Zie ook pagina 14 van de gebruikersgids kmo's. Hierbij de link: https://www.rvo.nl/file/de-nieuwe-definitie-van-kmo

Vraag 3

Waarom moeten incidenten bij twee instanties worden gemeld?
Incidenten moeten worden gemeld bij de toezichthouder ("bevoegde autoriteit") en bij het CSIRT (Computer Security Incident Response Team) voor digitale diensten.
De meldingen bij deze instanties dienen elk een ander doel.

Incidenten moeten worden gemeld bij de toezichthouder Agentschap Telecom. De toezichthouder kan naar aanleiding hiervan in actie komen en controleren of de digitale dienstverlener zich aan de wet heeft gehouden. Zij kan door de gemelde incidenten ook inzicht krijgen waar er zich in de sector (nieuwe) risico's voordoen. Als bijvoorbeeld blijkt dat veel incidenten worden veroorzaakt tijdens onderhoudswerkzaamheden aan ict-systemen, dan kan de toezichthouder digitale dienstverleners waarschuwen hier extra alert op te zijn en adviseren voorzorgsmaatregelen te treffen. Zo vervult de toezichthouder ook een rol bij het voorkomen van incidenten.

Daarnaast moeten incidenten ook worden gemeld bij het CSIRT voor digitale diensten. Een CSIRT staat voor "Computer Security Incident Response Team (CSIRT)". Een incident (vanaf een bepaalde omvang) moet bij het CSIRT worden gemeld. Het CSIRT kan advies geven en ondersteuning bieden. Dat is gericht op het herstel. Het CSIRT kan ook andere ondernemingen waarschuwen en informatie verstrekken over risico's en incidenten, bijvoorbeeld wanneer een beveiligingslek in bepaalde software is gesignaleerd. Het CSIRT moet niet worden beschouwd als de ict-verlener die in uw organisatie het probleem komt verhelpen. Dat zal u zelf of uw ict-dienstverlener moeten doen. Wat een CSIRT aan ondersteuning en advies kan bieden hangt ook af van de oorzaak en de eventuele impact van een incident, dus dat zal per situatie worden bekeken. Het is niet de taak van het CSIRT om te controleren of een onderneming zich aan de wet heeft gehouden.

Het Agentschap Telecom en het CSIRT voor digitale diensten vallen onder het Ministerie van Economische Zaken en Klimaat.

Vraag 4

Wat houdt de meldplicht van incidenten in?
Alleen incidenten ongeacht de oorzaak die een schadelijk effect hebben op de beveiliging van uw ict-systemen moeten worden gemeld. Echter, niet elk incident met gevolgen voor de beveiliging van uw ict-systemen vallen onder de wet; er gelden drempelwaarden zodat alleen incidenten met aanzienlijke gevolgen moeten worden gemeld. Dat betekent dat kleine incidenten met amper gevolgen niet hoeven worden gemeld.

Vraag 5

Als er zich een incident voordoet, is meestal niet meteen duidelijk wat er aan de hand is of hoe ernstig het is/wordt. Dan is ook niet duidelijk of het incident onder de meldplicht valt. Moet er dan ook al worden gemeld?
Twijfelt u of er moet worden gemeld, dan kunt u ook contact opnemen met het CSIRT en/of Agentschap Telecom om de situatie te bespreken.
Indien u alvast een melding wilt doen, maar nog niet over alle benodigde gegevens beschikt, kunt u ook op een later moment de resterende informatie aanvullen of de melding intrekken indien het incident veel kleiner of minder ernstig blijkt te zijn dan u aanvankelijk had ingeschat.

Vraag 6

Wat houdt de zorgplicht in?

De zorgplicht houdt in dat een digitale dienstverlener organisatorische en technische maatregelen moet nemen om de risico's voor de beveiliging van zijn netwerk- en informatiesystemen te beheersen. De wet gaat vooral in op wat u moet regelen (beveiligingselementen) maar schrijft niet voor hoe u dat moet doen en op welk beveiligingsniveau u dat moet doen. Dat is uw eigen verantwoordelijkheid. Dat betekent dat u goed inzicht moet hebben in de mogelijke risico's ten aanzien van de beveiliging van netwerk- en informatiesystemen. En de maatregelen zorgen voor een niveau van beveiliging dat is afgestemd op de risico's die zich voordoen. Het gaat hierbij bijvoorbeeld om het systematische beheer van uw ict-systemen en het beheer van bedrijfscontinuïteit.

Vraag 7

Gelden deze regels ook voor mijn concurrenten in andere EU landen?

Ja, in de andere EU lidstaten gelden dezelfde drempelwaarden voor de meldplicht en dezelfde beveiligingseisen. Deze drempelwaarden en beveiligingseisen zijn namelijk in een Europese Uitvoeringsverordening opgenomen en die is van kracht in alle EU-lidstaten.

Hierbij de link naar deze Uitvoeringsverordening (EU) 2018/151:
https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ%3AC%3A2018%3A151%3AFULL

Deze brochure is een uitgave van:

Ministerie van Economische Zaken en Klimaat
Postbus 20401 | 2500 EK Den Haag
T 070 379 89 11

September 2018 | 115815