CENTRE FOR
CYBER SECURITY
BELGIUM

GIDS VOOR DE MELDING VAN NIS-INCIDENTEN

DIGITALE DIENSTVERLENERS (DDV)

(“DIGITAL SERVICE PROVIDERS” - DSP)

CENTRUM VOOR
CYBERSECURITY BELGIË
Wetstraat 16
1000 Brussel

nis@ccb.belgium.be
www.ccb.belgium.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

.be

CENTRE FOR CYBER SECURITY BELGIUM

Opgelet:

Deze gids wil een antwoord bieden op de voornaamste vragen in verband met de melding door NIS-digitaledienstverleners in België.

Deze gids is evenwel niet exhaustief en ontheft digitaledienstverleners niet van de verplichting om de relevante algemene of sectorale wettelijke bepalingen na te gaan.

Inhoudsopgave

A. Lexicon 3

B. Wat is een digitaledienstverlener (DDV)? 6

C. Melding van NIS-incidenten door DDV's 13

1. Welke gebeurtenissen moeten verplicht door een DDV worden gemeld? *13*
2. Binnen welke termijn moet een incident worden gemeld? *16*
3. Aan wie moet de digitaledienstverlener het incident melden? *16*
4. Hoe moet de digitaledienstverlener het incident melden? *17*
5. Welke informatie moet de digitaledienstverlener bezorgen? *18*
6. Wat zijn de verschillende meldingsfasen bij een incident? *19*
7. Welke vertrouwelijkheidsregels zijn van toepassing op de informatie over een NIS-incident? *21*
8. Wat moet de digitaledienstverlener doen indien een NIS-incident ook een inbreuk in verband met persoonsgegevens is (AVG)? *22*

D. Bijlage 24

E. Sancties 27

F. Technische bijstand **28**

G. NIS-contactpunten **30**

H. Wettelijke referenties **31**

A. Lexicon

"Beveiliging van netwerk- en informatiesystemen"*: het vermogen van netwerk- en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen.*

"Centrum voor Cybersecurity België (CCB)": *federale overheidsdienst onder het rechtstreekse gezag van de Eerste Minister, opgericht bij het koninklijk besluit van 10 oktober 2014 (B.S., 21 november 2014, blz. 91395 e.v.).*

"Computer Emergency Response Team (CERT.be)": *operationele computer security incident response dienst van het Centrum voor Cybersecurity België.*

"Contactpunt voor de beveiliging van netwerk- en informatiesystemen"*: het contactpunt aangewezen door de digitaledienstverlener dat de functie van contactpunt uitoefent ten aanzien van het CCB, het NCCN en de sectorale overheid, voor elke vraag in verband met de beveiliging van de netwerk- en informatiesystemen van zijn digitale diensten opgesomd in bijlage II van de wet van 7 april 2019.*

***"Incident"**: elke gebeurtenis met een reële negatieve impact op de beveiliging van netwerk- en informatiesystemen.*

***"Incidentenbehandeling"**: alle procedures ter ondersteuning van de opsporing, analyse en beheersing van en reactie op een incident.*

***"Koninklijk NIS-besluit"**: het koninklijk besluit van 12 juli 2019 tot uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren (B.S., 18 juli 2019, blz. 72187 e.v.).*

***"Meldingsplatform"**: het platform voor het melden van incidenten bedoeld in artikel 31 van de wet van 7 april 2019.*

***"Nationaal Crisiscentrum (NCCN)"**: Algemene Directie van de Federale Overheidsdienst Binnenlandse Zaken, opgericht bij het koninklijk besluit van 18 april 1988 (B.S., 4 mei 1988, blz. 6408 e.v.).*

***"Nationaal CSIRT"**: het nationale computer security incident response team, namelijk het Centrum voor Cybersecurity België (CCB), opgericht bij het koninklijk besluit van 10 oktober 2014.*

***"Netwerk- en informatiesysteem"**:*

a) een elektronische-communicatienetwerk in de zin van artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;
b) een apparaat of groep van permanent of tijdelijk gekoppelde of bij elkaar behorende apparaten, waarvan een of meer elementen, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische componenten van dat apparaat

die met name de automatisering van het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken;
c) of digitale gegevens die via in de bepalingen onder a) en b), bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan.

***"NIS-wet"**: de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (B.S., 3 mei 2019, blz. 42857 e.v.).*

***"Risico"**: elke redelijkerwijs vast te stellen omstandigheid of gebeurtenis met een mogelijke negatieve impact op de beveiliging van netwerk- en informatiesystemen.*

***"Sectorale overheid"**: de overheid die bevoegd is voor het toezicht op de DDV's opgenomen in bijlage II bij de wet van 7 april 2019, namelijk de federale Minister bevoegd voor Economie of, bij delegatie, de FOD Economie.*

***"Verordening EU 2016/679"**: de Europese Verordening 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming "AVG").*

B. Wat is een digitaledienstverlener (DDV)?

Een digitaledienstverlener (DDV)[1] is een rechtspersoon die een digitale dienst aanbiedt als bedoeld in bijlage II bij de NIS-wet, die zijn hoofdkantoor in België heeft[2] en die geen micro- of kleine onderneming is.

1. *Een digitale dienst*

Een "digitale dienst" is een dienst als bedoeld in artikel 1, lid 1, punt b), van de Europese richtlijn 2015/1535[3].

Deze bepaling heeft betrekking op elke dienst van de informatiemaatschappij, dat wil zeggen elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht.

i) "op afstand", een dienst die wordt geleverd zonder dat de partijen gelijktijdig aanwezig zijn;
ii) "langs elektronische weg", een dienst die wordt verzonden en ontvangen via elektronische apparatuur voor de verwerking (met inbegrip van digitale compressie) en de opslag van gegevens, en die geheel via draden, radio, optische middelen of andere elektromagnetische middelen wordt verzonden, doorgeleid en ontvangen;

---

[1] Art. 6, 20°, van de NIS-wet en art. 4, 18), van de "NIS"-richtlijn (richtlijn EU nr. 2016/1148 van 6 juli 2016).
[2] Art. 3, § 2, van de NIS-wet (hoofdkantoor of plaats waar de vertegenwoordiger van de DDV voor de Europese Unie gevestigd is).
[3] Europese Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij.

iii) “op individueel verzoek van een afnemer van diensten”, een dienst die op individueel verzoek via de transmissie van gegevens wordt geleverd.

2. *Als bedoeld in bijlage II bij de NIS-wet*

Bijlage II van de NIS-wet omvat drie soorten digitale diensten:

i) Cloudcomputerdienst (“*cloud computing service*”*)*

Een cloudcomputerdienst is een digitale dienst die “toegang mogelijk maakt tot een schaalbare en elastische pool van deelbare computercapaciteit”.[4]

“Computercapaciteit” heeft betrekking op capaciteit zoals netwerken, servers en andere infrastructuur, opslag, applicaties en diensten.[5]

Met “schaalbaar” wordt bedoeld: computercapaciteit die, ongeacht de geografische locatie van de capaciteit, op flexibele wijze door aanbieders van cloudcomputerdiensten wordt toegewezen teneinde met schommelingen in de vraag te kunnen omgaan.[6]

Met “elastische groep” wordt bedoeld: de computercapaciteit die afhankelijk van de vraag ter beschikking wordt gesteld en wordt vrijgegeven teneinde deze beschikbare capaciteit snel te kunnen verhogen en verlagen naargelang van het werkvolume.[7]

---

[4] Art. 6, 29°, van de NIS-wet en art. 4, 19), van de NIS-richtlijn.
[5] Zie overweging 17 van de NIS-richtlijn.
[6] Idem.
[7] Idem.

Met “gedeeld” wordt bedoeld: de computercapaciteit die ter beschikking wordt gesteld aan meerdere gebruikers die een gemeenschappelijke toegang tot de dienst hebben, maar waarbij de verwerking voor elke gebruiker afzonderlijk plaatsvindt, hoewel de dienst door middel van dezelfde elektronische uitrusting wordt verleend.[8]

Cloudcomputerdiensten bestrijken dus een breed scala aan activiteiten die volgens verschillende modellen kunnen worden verricht.[9]

Momenteel bestaan er drie belangrijke soorten modellen van cloudcomputerdiensten die een aanbieder kan verstrekken[10]:

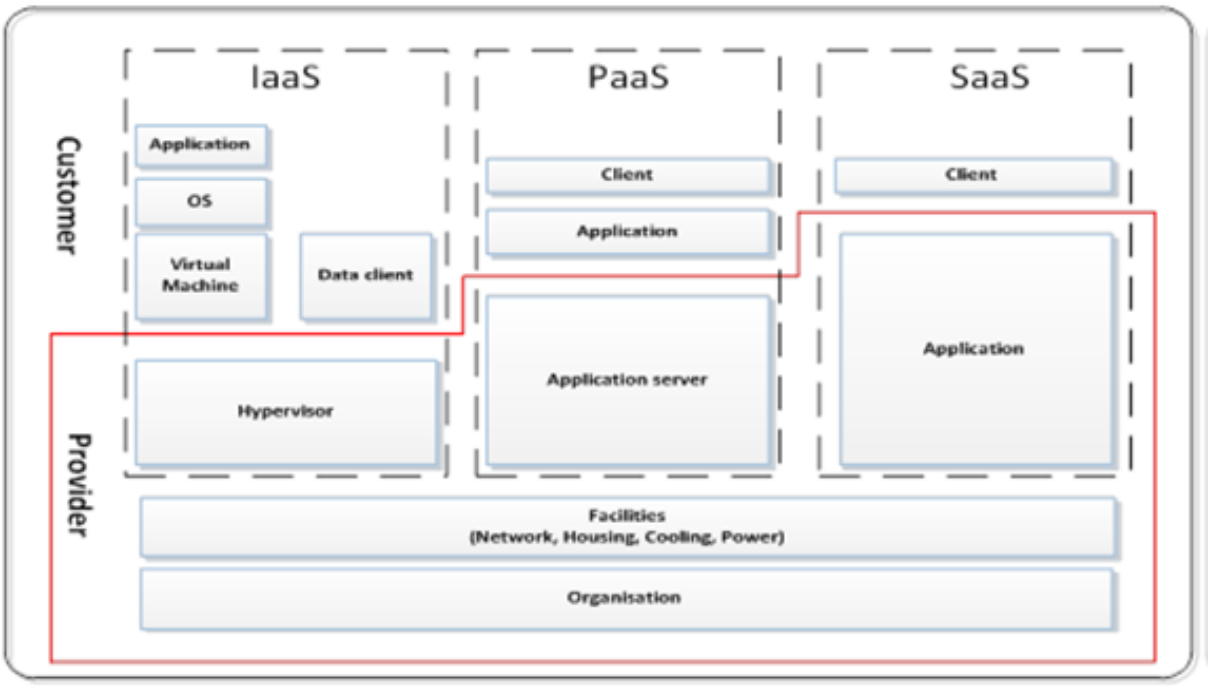
> ***Infrastructuur als dienst (“Infrastructure as a Service – IaaS”)*:** het soort cloudcapaciteit dat aan de klant wordt geboden, is een infrastructuur. Deze omvat onder meer de virtuele levering van computercapaciteit in de vorm van hardware-, netwerk- en opslagdiensten. IaaS bedient server-, opslag-, netwerk- en besturingssystemen. Er wordt ondernemingsinfrastructuur geboden waarin een onderneming haar gegevens kan opslaan en de applicaties kan draaien die nodig zijn voor haar dagelijkse werking.

---

[8] Idem.
[9] Idem.
[10] Bijlage bij de Mededeling van de Europese Commissie van 13.9.2017 (COM/2017/0476) “De NIS-richtlijn ten volle benutten – *naar de doeltreffende uitvoering van Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie*” (https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex:52017DC0476); Europees Parlement, “Cloud computing – An overview of economic and policy issues”, mei 2016 (https://www.europarl.europa.eu/RegData/etudes/IDAN/2016/583786/EPRS_IDA(2016)583786_EN.pdf).

Platform als dienst ("Platform as a Service – PaaS"): het soort cloudcapaciteit dat aan de klant wordt geboden, is een platform. Deze omvat onder meer onlinecomputerplatforms waarop ondernemingen bestaande applicaties kunnen draaien of nieuwe applicaties kunnen ontwikkelen en testen.

Software als dienst ("Software as a service – SaaS"): het soort cloudcapaciteit dat aan de klant wordt geboden, is een applicatie of computersoftware die over het internet is opgezet. Dit type clouddiensten maakt dat het voor de eindgebruiker niet meer noodzakelijk is software te kopen, te installeren en te beheren, en heeft het voordeel dat de software door middel van een internetverbinding van op om het even welke plaats toegankelijk kan worden gesteld.



(Dienstverleningsmodellen en activa in cloud computing) [11]

[11] Bijlage bij de Mededeling van de Europese Commissie van 13.9.2017 (COM/2017/0476), p. 35 (Asset in cloud computing - https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes)

ii) Onlinemarktplaats ("online marketplace")

Een onlinemarktplaats is een digitale dienst die het consumenten[12] en/of ondernemingen[13] mogelijk maakt online verkoop- of dienstenovereenkomsten met ondernemingen te sluiten op de website van de onlinemarktplaats of op de website van een onderneming die gebruikmaakt van door de onlinemarktplaats aangeboden informaticadiensten.[14]

Een onlinemarktplaats maakt het consumenten en ondernemers mogelijk online verkoop- of dienstenovereenkomsten met ondernemers te sluiten en is de eindbestemming voor het sluiten van deze overeenkomsten.[15]

Dit begrip omvat geen onlinediensten die slechts als tussenschakel voor diensten van een derde fungeren waarmee uiteindelijk een overeenkomst kan worden gesloten. Het heeft dus geen betrekking op onlinediensten die de prijzen van bepaalde producten of diensten van verschillende ondernemers vergelijken en die de gebruiker vervolgens automatisch naar de geprefereerde ondernemer doorverwijzen om het product te kopen.[16]

Tot de computerdiensten die op de onlinemarktplaats worden aangeboden, kunnen de verwerking van transacties, de verzameling van gegevens of de profilering van gebruikers behoren (bijvoorbeeld, applicatiewinkels, die de digitale distributie van applicaties of softwareprogramma's van derden mogelijk maken).[17]

---

[12] Als bedoeld in artikel I.1., eerste lid, 2°, van het Wetboek van economisch recht.
[13] Als bedoeld in artikel I.8, 39°, van het Wetboek van economisch recht.
[14] Art. 6, 27°, van de NIS-wet en art. 4, 17), van de "NIS"-richtlijn (richtlijn EU nr. 2016/1148 van 6 juli 2016).
[15] Zie overweging 15 van de NIS-richtlijn.
[16] Idem.
[17] Idem. Een aanbieder als eBay bijvoorbeeld kan worden beschouwd als een onlinemarktplaats omdat deze anderen de mogelijkheid biedt op zijn platform winkels op te zetten om producten en diensten online beschikbaar te stellen aan

iii) Een onlinezoekmachine ("online search engine")

Een onlinezoekmachine is een digitale dienst die het gebruikers mogelijk maakt zoekacties uit te voeren op in principe alle websites of websites in een bepaalde taal op basis van een zoekvraag over om het even welk onderwerp in de vorm van een trefwoord, een zin of andere input; het resultaat zijn hyperlinks naar informatie over de opgevraagde inhoud.[18]

De definitie van een onlinezoekmachine heeft geen betrekking op zoekfuncties die beperkt zijn tot de inhoud van een specifieke website, ongeacht of de zoekfunctie door een externe zoekmachine wordt aangeboden. [19] Zij heeft evenmin betrekking op onlinediensten die de prijzen van bepaalde producten of diensten van andere ondernemers vergelijken en die de gebruiker vervolgens automatisch doorverwijzen naar de geprefereerde ondernemer om het product te kopen.[20]

3. *Die geen micro- of kleine onderneming is*

Micro- of kleine ondernemingen, als bedoeld in de aanbeveling van de Europese Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen 2003/361/EG, zijn niet onderworpen aan de verplichtingen die voortvloeien uit de NIS-wet:

---

consumenten of bedrijven (zie Bijlage bij de Mededeling van de Europese Commissie van 13.9.2017 (COM/2017/0476), p. 33).

[18] Art. 6, 28°, van de NIS-wet en art. 4, 17), van de NIS-richtlijn.

[19] Overweging 16 van de NIS-richtlijn en Bijlage bij de Mededeling van de Europese Commissie van 13.9.2017 (COM/2017/0476), p. 33.

[20] Idem.

Kleine onderneming[21]	onderneming waar **minder dan 50 personen** werkzaam zijn **en** waarvan de jaaromzet (of het jaarlijkse balanstotaal) **10 miljoen euro niet overschrijdt**. - **beide voorwaarden zijn cumulatief**
Micro-onderneming[22]	onderneming waar **minder dan 10 personen** werkzaam zijn **en** waarvan de jaaromzet (of het jaarlijkse balanstotaal) **2 miljoen euro niet overschrijdt**. - **beide voorwaarden zijn cumulatief**

De rechtspersoon moet m.a.w. enerzijds meer dan 50 personen tewerkstellen en anderzijds een jaaromzet (of jaarlijks balanstotaal) van meer dan 10 miljoen euro hebben om te worden beschouwd als een digitaledienstverlener in de zin van de NIS-wet.

C. Melding van NIS-incidenten door DDV's

1. Welke gebeurtenissen moeten verplicht door een DDV worden gemeld?

Een Belgische NIS-digitaledienstverlener (zie punt B) moet **alle incidenten melden die aanzienlijke gevolgen hebben voor de verlening van de door hem in de Europese Unie aangeboden digitale dienst(en)**.[23]

[21] Art. 2 (2.) Aanbeveling van de Europese Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen 2003/361/EG.
[22] Art. 2 (3.) Aanbeveling van de Europese Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen 2003/361/EG.
[23] Art. 35, §§ 1 en 3, van de NIS-wet.

Een incident is elke gebeurtenis met een reële negatieve impact op de beveiliging van netwerk- en informatiesystemen.[24]

De beveiliging van netwerk- en informatiesystemen is het vermogen van netwerk- en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen.[25]

De Europese Commissie heeft de gevallen vastgesteld waarin een incident duidelijk aanzienlijke gevolgen heeft voor de verlening van een digitale dienst in de Unie (Uitvoeringsverordening nr. 2018/151 van 30 januari 2018):

Duur van het incident: ***onbeschikbaarheid gedurende meer dan 5.000.000 gebruikersuren***	- met ***de duur*** wordt de tijdspanne bedoeld vanaf het moment dat de dienst niet meer naar behoren werkt op het vlak van beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid, tot het moment van volledig herstel van de dienst; - het begrip ***gebruikersuur*** verwijst naar het aantal gebruikers in de Europese Unie dat getroffen is voor een tijdspanne van zestig minuten.

[24] Art. 6, 13°, van de NIS-wet.
[25] Art. 6, 8° en 9°, van de NIS-wet.

Aantal gebruikers: ***meer dan 100.000 getroffen gebruikers***	- tot de ***gebruikers*** van digitale diensten behoren alle natuurlijke en rechtspersonen die klant of abonnee zijn van een onlinemarktplaats of cloudcomputerdienst, of die op de website van een onlinezoekmachine aan de hand van trefwoorden zoekopdrachten uitvoeren.
Aard van de impact: ***risico voor de openbare veiligheid*** ***of risico voor de openbare beveiliging*** ***of heeft geleid tot een risico van verlies van mensenlevens***	- de DDV kan de aard van de impact bepalen op basis van indicaties zoals de aard van zijn contractuele betrekkingen met de klant of, in voorkomend geval, het potentiële aantal getroffen gebruikers.
Materiële schade: ***veroorzaakte schade > 1.000.000 €***	- het incident veroorzaakt voor minstens één gebruiker in de Europese Unie schade **>** ***1.000.000 €***

Opgelet:

De drempels vermeld in de uitvoeringsverordening van de Europese Commissie van 30 januari 2018 (nr. 2018/151) mogen niet worden beschouwd als een limitatieve lijst van incidenten die aanzienlijke gevolgen hebben voor de verlening van een digitale dienst: het betreft louter een lijst met duidelijke gevallen waarin een incident moet worden geacht aanzienlijke gevolgen te hebben voor de verlening van een digitale dienst.

De digitaledienstverlener blijft verantwoordelijk om te bepalen of het incident al dan niet aanzienlijke gevolgen heeft, onder het toezicht, achteraf, van de inspectiedienst van de FOD Economie.

Los van voornoemde drempels en parameters worden digitaledienstverleners aangemoedigd om op vrijwillige basis ieder incident met voorheen onbekende kenmerken te melden, zoals nieuwe aanvalsvectoren, dreigingen, gevaren of zwakke punten.

2. Binnen welke termijn moet een incident worden gemeld?

De DDV moet het incident onverwijld melden, dat wil zeggen zo vlug mogelijk.[26]

De verplichting om een incident te melden geldt alleen vanaf het ogenblik dat de digitaledienstverlener toegang heeft tot de informatie die nodig is om de gevolgen van een incident volledig of gedeeltelijk te beoordelen.[27]

3. Aan wie moet de digitaledienstverlener het incident melden?

a) De digitaledienstverlener moet het incident tegelijkertijd aan drie overheden melden[28]:

- het Centrum voor Cybersecurity België (CCB – dienst CERT.be);
- het Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken (NCCN);

[26] Art. 35, § 1, van de NIS-wet.
[27] Art. 35, § 3, van de NIS-wet.
[28] Art. 35, § 1, van de NIS-wet.

- de FOD Economie (sectorale overheid).

In de praktijk wordt het incident in één keer gemeld door het formulier op het NIS-meldingsplatform in te vullen. De informatie wordt dan via het platform automatisch naar de drie betrokken overheden gestuurd.

b) De DDV die een digitale dienst verleent aan een AED moet de betrokken AED (zijn klant) ook onverwijld alle incidenten melden die verband houden met de aan die AED verleende digitale dienst(en) en die aanzienlijke gevolgen hebben voor de continuïteit van de essentiële diensten van de betrokken AED.

Vervolgens moet de AED het incident melden volgens de meldingsprocedures voor AED's.

4. Hoe moet de digitaledienstverlener het incident melden?

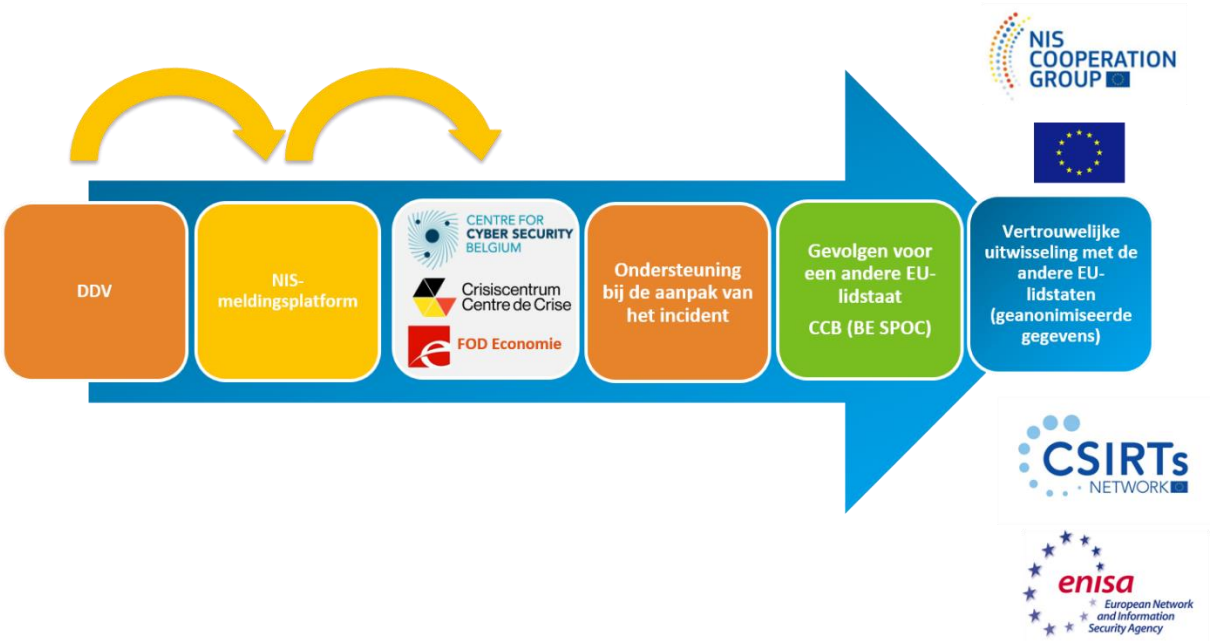
De digitaledienstverlener moet het incident melden via het NIS-meldingsplatform[29]: ***https://nis-incident.be***

De DDV moet de FOD Economie (nis-dsp@economie.fgov.be) vragen een account aan te maken (gebruikersnaam/wachtwoord) om toegang te krijgen tot het NIS-meldingsplatform.

Het platform is toegankelijk via internet door middel van een beveiligde verbinding en een voor elke digitaledienstverlener unieke identificatiesleutel.[30]

[29] Art. 36 van de NIS-wet en art. 8 van het NIS-KB.
[30] Art. 7 van het NIS-KB.

Melding van NIS-incidenten DDV



Indien het NIS-meldingsplatform niet beschikbaar is, moet de DDV het incident melden volgens de modaliteiten vermeld op de website van het CCB (https://cert.be/nl/een-incident-melden-form).

5. Welke informatie moet de digitaledienstverlener bezorgen?

De digitaledienstverlener gebruikt het formulier voor het melden van incidenten dat op het NIS-meldingsplatform beschikbaar is: *https://nis-incident.be/*

De melding omvat alle beschikbare informatie die toelaat de aard, de oorzaken, de effecten en de gevolgen van het incident te bepalen[31]:

a) de naam en contactgegevens van de digitaledienstverlener en de door hem verleende digitale dienst;
b) de datum en het tijdstip waarop het incident plaatsvond;
c) de duur van het incident;
d) de omvang van het geografische gebied dat door het incident is getroffen en de eventuele grensoverschrijdende aard ervan;
e) het aantal getroffen gebruikers;
f) informatie over de aard van het incident;
g) de omvang van de gevolgen van het incident, met name voor maatschappelijke en economische activiteiten;
h) het belang van de systemen of van de betrokken informatie;
i) de gevolgen van het incident voor in België gevestigde internationale organisaties;
j) de ondernomen acties;
k) de beschrijving van de huidige situatie.

6. Wat zijn de verschillende meldingsfasen bij een incident?

De digitaledienstverlener moet het CCB en de FOD Economie op de hoogte houden van de evolutie van het incident en de ondernomen remediërende acties.

[31] Art. 8, § 1, van het NIS-KB.

Wanneer de digitaledienstverlener niet alle in het formulier gevraagde informatie kan verstrekken met behulp van de gegevens waarover hij beschikt, vult hij de oorspronkelijke melding via het meldingsplatform aan zodra de ontbrekende informatie beschikbaar is.[32]

Hij doet dit eveneens in geval van nieuwe informatie of belangrijke ontwikkelingen.[33]

Op verzoek van het CCB, het NCCN, de FOD Economie meldt de digitaledienstverlener via het meldingsplatform een actualisering van het meldingsformulier waarin hij de behandeling van het incident beschrijft vanaf het ontdekken tot het afsluiten ervan en alle informatie van het meldingsformulier overneemt.[34]

De meldingsprocedure kan verschillende fasen omvatten:

a) De ***initiële melding*** moet onverwijld plaatsvinden, zelfs indien de DDV nog niet over alle relevante informatie beschikt. Doel van deze initiële melding is het CCB, de FOD Economie, en het NCCN te wijzen op het incident en de mogelijke gevolgen ervan.

b) ***Bijkomende meldingen***[35] moeten regelmatig worden verstuurd of zodra de DDV over nieuwe informatie beschikt. Doel van deze bijkomende meldingen is het CCB, de FOD Economie, en het NCCN op de hoogte te houden van de status van het incident. De DDV doet dan een nieuwe melding op het platform, waarbij hij enkel de nieuwe gegevens en het referentienummer van de initiële melding vermeldt.

---

[32] Art. 8, § 2, van het NIS-KB.
[33] Art. 8, § 3, van het NIS-KB.
[34] Art. 8, § 4, van het NIS-KB.
[35] Art. 8, § 3, van het NIS-KB.

c) Een ***eventueel eindverslag*** (op verzoek van een van de voornoemde overheden) met alle informatie die naar het CCB, de FOD Economie, en het NCCN is gestuurd. Doel van dit eindverslag is een overzicht te geven van het incident en er conclusies uit te trekken.

De DDV moet het CCB, het NCCN en de FOD Economie, op de hoogte houden van de evolutie van het incident en de ondernomen remediërende acties.

Het CCB, de FOD Economie en het NCCN kunnen de digitaledienstverlener bijkomende informatie vragen over diens meldingen.

Wanneer de omstandigheden dit toelaten, verstrekt het CCB de digitaledienstverlener die de melding heeft gedaan, alle informatie die nuttig is voor de opvolging van diens melding, en, in voorkomend geval, alle informatie die kan bijdragen tot een doeltreffende behandeling van het incident.[36]

7. Welke vertrouwelijkheidsregels zijn van toepassing op de informatie over een NIS-incident?

De DDV en zijn onderaannemers beperken de toegang tot de informatie over incidenten tot de personen die deze informatie nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met de NIS-wet.[37]

Deze regel geldt ook voor het CCB (nationaal CSIRT), het NCCN en de FOD Economie.

[36] Art. 10 van het NIS-KB.
[37] Art. 9, § 1, van de NIS-wet.

De personeelsleden van de digitaledienstverlener en zijn onderaannemers zijn gebonden aan het beroepsgeheim wat de informatie over een NIS-incident betreft.[38]

De informatie die door een digitaledienstverlener aan het CCB, het NCCN en de FOD Economie wordt bezorgd, mag worden uitgewisseld met autoriteiten van de Europese Unie, en met andere Belgische of buitenlandse autoriteiten, wanneer die uitwisseling noodzakelijk is voor de toepassing van wettelijke bepalingen.

Deze informatieoverdracht wordt evenwel beperkt tot hetgeen relevant is voor en evenredig is met het doel van die uitwisseling, overeenkomstig Verordening EU 2016/679, de vertrouwelijkheid van de betrokken informatie, alsook de veiligheid en de commerciële belangen van de digitaledienstverlener.[39]

8. Wat moet de digitaledienstverlener doen indien een NIS-incident ook een inbreuk in verband met persoonsgegevens is (AVG)?

Naargelang de ingevoerde informatie wordt de DDV met een standaardbericht ingelicht over zijn verplichting om eventuele inbreuken in verband met persoonsgegevens[40] te melden aan een van de "toezichthoudende autoriteiten" met behulp van de geschikte meldingstools (bijvoorbeeld: https://www.gegevensbeschermingsautoriteit.be/meldformulier-voor-gegevenslekken).

[38] Art. 9, § 2, van de NIS-wet.
[39] Art. 9, § 3, van de NIS-wet.
[40] Art. 33, eerste alinea, van verordening EU 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

Bijzondere regels betreffende persoonsgegevens

Voor de verwerking van persoonsgegevens door een DDV in het kader van de NIS-wet kan eventueel worden afgeweken van de artikelen 12 tot 22 van de Algemene Verordening Gegevensbescherming "AVG" (*Verordening (EU) 2016/679 Hoofdstuk III - Rechten van de betrokkene).* De vrijstelling geldt, onder voorbehoud van het evenredigheidsbeginsel en in voorkomend geval van het beginsel van minimale gegevensverwerking, voor alle categorieën van persoonsgegevens, voor zover de verwerking van deze gegevens in overeenstemming is met het doeleinde van de verwerking (bijvoorbeeld de melding van een incident) en noodzakelijk is voor dit doeleinde.[41]

De gegevens (met inbegrip van de persoonsgegevens) worden door de DDV niet langer bewaard dan nodig is voor de doeleinden van de wet, met een maximale bewaartermijn die de duur van de verjaringstermijn van eventuele inbreuken bedoeld in de artikelen 51, § 1 en 52, § 2, van de NIS-wet niet mag overschrijden.[42]

[41] Art. 71, § 2 en § 4, van de NIS-wet.
[42] Art. 71, § 5, van de NIS-wet.

D. Bijlage

Uittreksel uit de Uitvoeringsverordening van de Europese Commissie van 30 januari 2018 (nr. 2018/151):

Artikel 3

In aanmerking te nemen parameters om te bepalen of een incident aanzienlijke gevolgen heeft

"1. Wat betreft het aantal gebruikers dat door het incident wordt getroffen, in het bijzonder gebruikers die de dienst nodig hebben voor de verlening van hun eigen diensten, als bedoeld in artikel 16, lid 4, onder a), van Richtlijn (EU) 2016/1148, is de digitaledienstverlener in staat het volgende ramen [sic]:

a) het aantal getroffen natuurlijke personen en rechtspersonen waarmee een dienstenovereenkomst is gesloten, of;

b) het aantal getroffen gebruikers van de dienst op basis van eerdere internetverkeersgegevens.

2. Met de duur van een incident als bedoeld in artikel 16, lid 4, onder b) van Richtlijn (EU) 2016/1148 wordt de tijdspanne bedoeld vanaf het moment dat de dienst niet meer naar behoren werkt op het vlak van beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid, tot het moment van volledig herstel van de dienst.

3. Wat betreft de omvang van het geografische gebied dat door het incident is getroffen, als bedoeld in artikel 16, lid 4, onder c), van Richtlijn (EU) 2016/1148, is de digitaledienstverlener in staat na te gaan of het incident gevolgen heeft voor zijn dienstverlening in specifieke lidstaten.

4. De omvang van de verstoring van de werking van de dienst als bedoeld in artikel 16, lid 4, onder d), van Richtlijn (EU) 2016/1148, wordt gemeten met betrekking tot een of meer van de volgende kenmerken die in het gedrang komen door een incident: de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van de gegevens of de daaraan gerelateerde diensten.

5. Wat betreft de omvang van de impact op de economische en maatschappelijke activiteiten als bedoeld in artikel 16, lid 4, onder e), van Richtlijn (EU) 2016/1148, is de digitaledienstverlener in staat om op basis van indicaties zoals de aard van zijn contractuele betrekkingen met de klant of, in voorkomend geval, het potentiële aantal getroffen gebruikers, te besluiten of het incident heeft geleid tot aanzienlijke materiële of immateriële schade voor de gebruikers, bijvoorbeeld op het vlak van gezondheid, veiligheid of schade aan eigendommen (…)".

Artikel 4

Aanzienlijke gevolgen van een incident

"1. Van een incident zal worden geacht dat het aanzienlijke gevolgen heeft indien minstens één van de volgende situaties heeft plaatsgevonden:

a) de door een digitaledienstverlener verleende dienst was gedurende meer dan 5 000 000 gebruikersuren onbeschikbaar, waarbij het begrip gebruikersuur verwijst naar het aantal gebruikers in de Unie dat getroffen is voor een tijdspanne van zestig minuten;

b) het incident heeft geleid tot een verlies aan integriteit, authenticiteit of vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die worden aangeboden door, of toegankelijk zijn via

een netwerk- en informatiesysteem van, [sic] de digitaledienstverlener, waarbij meer dan 100 000 gebruikers in de Unie zijn getroffen;

c) het incident heeft geleid tot een risico voor de openbare veiligheid, de openbare beveiliging <u>of</u> tot een risico van verlies van mensenlevens;

d) het incident heeft voor minstens één gebruiker in de Unie materiële schade veroorzaakt, waarbij de schade voor die gebruiker meer dan 1 000 000 EUR bedraagt (…)"

CENTRE FOR CYBER SECURITY BELGIUM

E. Sancties

Inbreuk	**Strafrechtelijke sanctie** (per inbreuk)	**Administratieve sanctie** (per inbreuk)
Niet melden van een incident.	Gevangenisstraf van 8 dagen tot 1 jaar en strafrechtelijke geldboete van 208 € (26 € x 8 (*)) tot 160.000 € (20.000 € x 8 (*)) of een van deze twee straffen.	Administratieve geldboete van 500 tot 75.000 €
Niet naleven van de vertrouwelijkheid/het beroepsgeheim.	Gevangenisstraf van 1 jaar tot 3 jaar en strafrechtelijke geldboete van 800 € (100 € x 8 (*)) tot 8.000 € (1.000 € x 8 (*)) of een van deze twee straffen (zie art. 458 van het Strafwetboek).	
Iedere handeling waarbij een persoon nadelige gevolgen ondervindt wanneer hij te goeder trouw een incident meldt.		Administratieve geldboete van 500 tot 200.000 €
Herhaling	In geval van herhaling van dezelfde feiten binnen een termijn van drie jaar wordt de	In geval van herhaling van dezelfde feiten binnen een termijn van drie jaar wordt

	strafrechtelijke geldboete verdubbeld en de overtreder bestraft met een gevangenisstraf van 15 dagen tot 3 jaar.	de administratieve geldboete verdubbeld.

(*) toepasselijke opdeciemen voor de maand april 2020 – zie website van de FOD Justitie voor de huidige vermenigvuldigingscoëfficiënt van de opdeciemen.

F. Technische bijstand

Het CCB zorgt in de mate van het mogelijke voor een technische eerstelijnssupport voor de gebruikers van het platform.

Het technisch team van het CCB is bereikbaar:

- via e-mail: cert@cert.be
- telefonisch: +32 (0)2 501 05 60

Het BIPT zorgt in de mate van het mogelijke voor een technische tweedelijnssupport voor de gebruikers van het platform.

Het technisch team van het BIPT is bereikbaar:

- via e-mail: netsec@bipt.be
- telefonisch: +32 (0)2 226 88 88

G. NIS-contactpunten

CENTRUM VOOR CYBERSECURITY BELGIË (CCB)
Wetstraat 16
1000 Brussel

NIS Team	nis@ccb.belgium.be	+32 (0)2 501 02 11	www.ccb.belgium.be
CERT.be Team	cert@cert.be	+32 (0)2 501 05 60	www.cert.be

FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN (FOD)
NATIONAAL CRISISCENTRUM (NCCN)
Hertogstraat 53
1000 Brussel
https://crisiscentrum.be/nl/contact

FEDERALE OVERHEIDSDIENST (FOD) ECONOMIE, K.M.O., MIDDENSTAND EN ENERGIE
Algemene Directie Kwaliteit en Veiligheid
Metrologie – Dienst Reglementering Metrologie Digital Trust
Koning Albert II-laan 16
1000 Brussel

nis-dsp@economie.fgov.be

+32 0800 120 33 (contact center)

H. Wettelijke referenties

- Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (*B.S.*, 3 mei 2019, blz. 42857 e.v.) – “NIS-wet”.

- Koninklijk besluit van 12 juli 2019 tot uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren (*B.S.*, 18 juli 2019, blz. 72187 e.v.) – “NIS-KB”.

- Uitvoeringsverordening van de Commissie van 30 januari 2018 (nr. 2018/151) tot vaststelling van toepassingsbepalingen voor Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad wat betreft de nadere specificatie van de door digitaledienstverleners in aanmerking te nemen elementen voor het beheer van de risico's in verband met de beveiliging van netwerk- en informatiesystemen en van de parameters om te bepalen of een incident aanzienlijke gevolgen heeft.

- Verordening EU 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Algemene Verordening Gegevensbescherming “AVG”).

- Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (*B.S.*, 5 september 2018, blz. 68616 e.v.).

CENTRE FOR
CYBER SECURITY
BELGIUM

GIDS VOOR DE MELDING VAN INCIDENTEN – NIS DIGITALEDIENSTVERLENERS (DDV'S)

Dit document en de bijlagen werden opgesteld door het Centrum voor Cybersecurity België (CCB). Deze federale overheidsinstelling werd opgericht bij het koninklijk besluit van 10 oktober 2014 en staat onder het gezag van de Eerste Minister.

Alle teksten, lay-out, ontwerpen en overige elementen van welke aard ook in dit document zijn onderworpen aan de wetgeving op de auteursrechten. Uittreksels uit dit document mogen alleen voor niet-commerciële doeleinden en met bronvermelding worden gereproduceerd.

Het CCB wijst alle aansprakelijkheid in verband met de inhoud van dit document af.

De vermelde informatie:
• is louter algemeen van aard en heeft niet tot doel alle specifieke situaties te behandelen;
• is niet noodzakelijk op alle vlakken volledig, nauwkeurig of up-to-date.

Verantwoordelijke uitgever:
Centrum voor Cybersecurity België
M. De Bruycker, Directeur
Wetstraat 16
1000 Brussel

Wettelijk depot:
D/2020/14828/007

2020