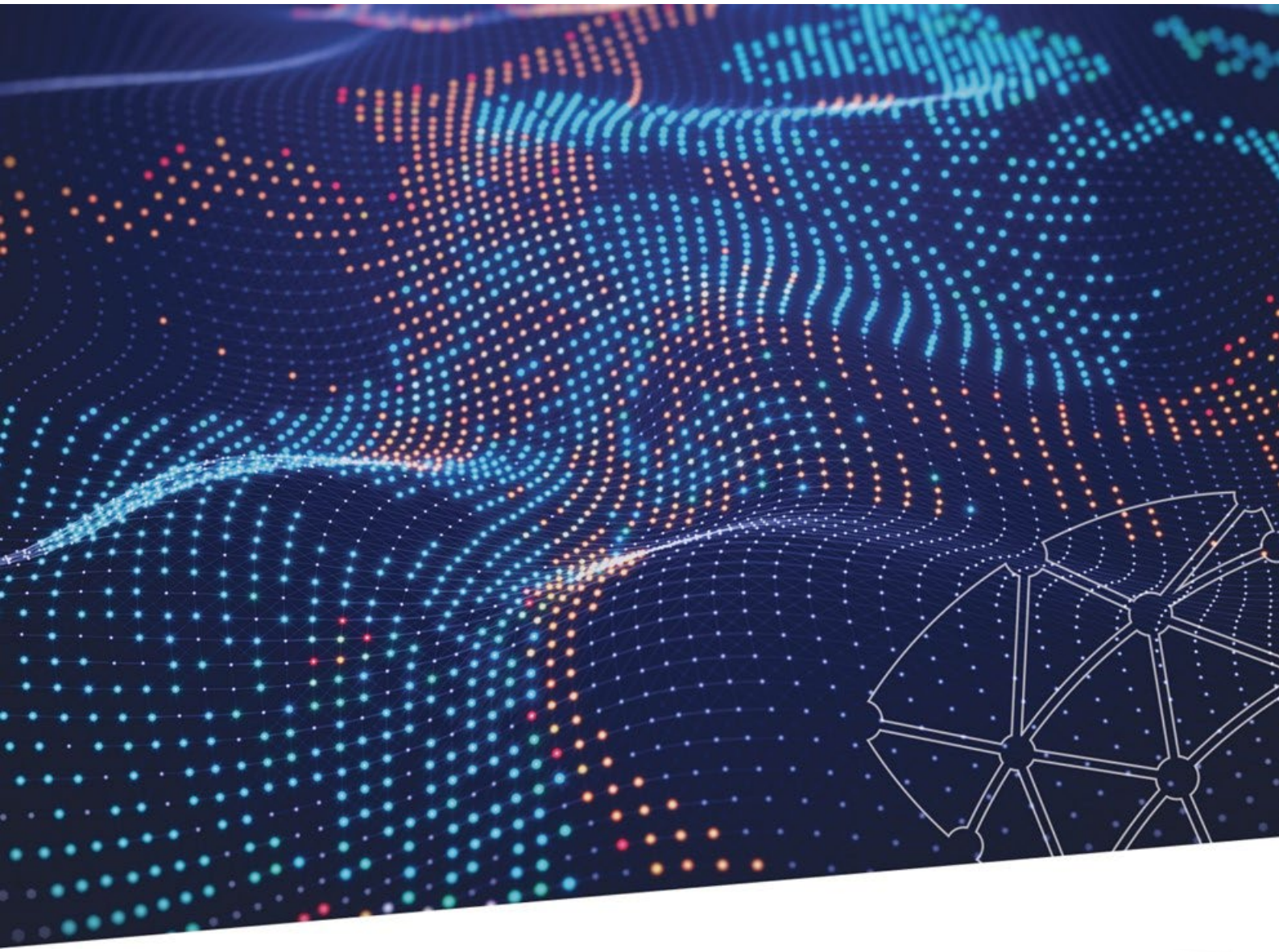
CENTRE FOR CYBERSECURITY BELGIUM



GIDS VOOR NIS2 MELDINGEN

Versie 10.2024 – 1.1

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Inleiding

De wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (de "NIS2-Wet") zet de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 om (de "NIS2-richtlijn").

Om het groeiende cyberdreigingslandschap en nieuwe uitdagingen het hoofd te bieden, heeft de Europese Unie nieuwe regelgeving aangenomen betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (de Richtlijn (EU) 2022/2555 van 14 december 2022- de "NIS2-richtlijn"), die de "NIS1-richtijn" vervangt (Richtlijn 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie).

Een van de belangrijkste verplichtingen die voortvloeit uit de NIS2-richtlijn en de NIS2-wet is de informatie- en meldingsverplichting voor incidenten. Deze verplichting is bedoeld om bijstand te verlenen aan de betrokken entiteiten, om de verschillende bevoegde autoriteiten adequaat te informeren, om waarschuwingen over bepaalde dreigingen te verspreiden onder andere entiteiten en om samen te werken op nationaal of Europees niveau.

Dit document is bedoeld om algemene informatie te verlenen over het melden van incidenten en de informatieverplichting in het kader van de NIS2-wet, die op 18 oktober 2024 van kracht worden.

Inhoudstafel

A. De verplichte meldingen

A.1. WELKE GEBEURTENISSEN MOETEN VERPLICHT GEMELD WORDEN DOOR ENTITEITEN DIE ONDER DE NIS2-WET VALLEN?

Een gebeurtenis dient verplicht gemeld te worden als het om een “significant” incident gaat. Dit impliceert twee zaken.

Ten eerste dient er sprake te zijn van **een incident**, zoals gedefinieerd in art. 8, 5° van de NIS2-wet: "een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt".

Ten tweede moet het incident **een significant incident**, zoals gedefinieerd in art. 8, 57° van de NIS2-wet uitmaken: "elk incident dat significante gevolgen heeft voor de verlening van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II van de wet en dat:

1° een ernstige operationele verstoring van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II of financiële verliezen voor de betrokken entiteit heeft veroorzaakt of kan veroorzaken; of
2° andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken."

A.2. HOE CONCREET BEPALEN OF EEN INCIDENT AL DAN NIET SIGNIFICANT IS?

Ten eerste moet het incident (zie definitie hierboven) gevolgen hebben voor de verlening van een van de diensten in de sectoren of deelsectoren opgesomd in bijlage I en II van de wet, d.w.z. **het moet gevolgen hebben op de netwerk- en informatiesystemen die de verlening van een of meer van deze dienst(en) ondersteunen** (bv. elektriciteitsdistributie).

De verplichte meldingen hebben daarom alleen betrekking op de informatiesystemen en -netwerken waarvan de betrokken entiteit afhankelijk is om de dienst(en) te verlenen die in de bijlagen bij de wet worden opgesomd. Een incident op een geïsoleerd informatiesysteem dat geen verband heeft met de levering van bovengenoemde diensten, hoeft dus niet te worden gemeld.

Bovendien moeten deze gevolgen significant zijn, namelijk het incident moet minstens een van de volgende drie situaties veroorzaken of kunnen veroorzaken:

- een **ernstige operationele verstoring van een van de geleverde diensten** (in de sectoren of subsectoren opgesomd in de bijlagen I en II van de NIS2-wet);
- **financiële verliezen voor de betrokken entiteit**;
- **aanzienlijke materiële, fysieke of morele schade aan andere natuurlijke personen of rechtspersonen**.

Om de entiteiten te ondersteunen in deze beoordeling, heeft het CCB hieronder enkele concrete situaties geïdentificeerd, waarin een entiteit een incident als significant zou moeten beoordelen.

De beschreven situaties zijn echter niet exhaustief of limitatief met betrekking tot de verschillende significante incidenten die zich kunnen voordoen.

1) Een vermoedelijk kwaadwillige gebeurtenis die de authenticiteit, integriteit, of vertrouwelijkheid van gegevens op de netwerk- en informatiesystemen van de entiteiten in gevaar brengt en die een ernstige operationele verstoring veroorzaakt of mogelijks kan veroorzaken.

Een dergelijke gebeurtenis kan zich voordoen wanneer (één van deze omstandigheden is voldoende) :

- iemand meer dan de voorziene toegangsrechten heeft verkregen tot de netwerken, systemen of informatie die de levering van de dienst(en) van de entiteit ondersteunen;
- een systeem of netwerk dat de levering van de dienst(en) van de entiteit ondersteunt, geconfigureerd is of kan worden door een persoon die niet de rechten zou mogen hebben om het systeem of netwerk van

de entiteit te configureren;
- een systeem of netwerk dat de levering van de dienst(en) van de entiteit ondersteunt, niet langer kan worden geconfigureerd door bevoorrechte gebruikers die de rechten zouden moeten hebben om het systeem of netwerk te configureren;
- de configuraties of informatie van de systemen die de levering van de dienst(en) van de entiteit ondersteunen onrechtmatig zijn gewijzigd, verwijderd, toegevoegd of onbetrouwbaar gemaakt;
- een systeem of netwerk dat de levering van de dienst(en) van de entiteit ondersteunt taken uitvoert die het niet hoort uit te voeren, taken niet uitvoert die het hoort uit te voeren of taken niet uitvoert die het hoort uit te voeren in verband met de toegang tot of de integriteit van het systeem of netwerk.

Wanneer een kwaadwillende actor zich bijvoorbeeld op voorhand in het netwerk- en informatiesysteem van de betrokken entiteit positioneert, met de bedoeling om in de toekomst diensten te verstoren, dan moet het incident als significant worden beschouwd.

2) Een gebeurtenis die de beschikbaarheid van gegevens op de netwerk- en informatiesystemen van de entiteit in gevaar brengt en die een ernstige operationele verstoring veroorzaakt of mogelijks kan veroorzaken.

Een dergelijke gebeurtenis kan zich voordoen wanneer:

- minstens 20% van de gebruikers minstens één uur geen toegang heeft tot de dienst;
- gebruikers minstens een uur lang geen toegang hebben tot de dienst en de entiteit het aantal getroffen gebruikers niet kan vaststellen (in relatieve of absolute zin);
- de gebeurtenis een vertraging veroorzaakt in de levering van producten die de contractueel gegarandeerde levertijden overschrijdt;

Bij een geplande uitschakeling voor onderhoud, is er geen sprake van een incident op voorwaarde dat de impact beperkt blijft tot de impact die gepland was.

Het begrip ‘gebruiker’ moet worden opgevat als verwijzend naar natuurlijke personen en/of rechtspersonen, professionele klanten en/of eindklanten die een contract hebben gesloten met de betrokken entiteit waardoor ze toegang hebben tot de betreffende dienst of gegevens, en die de gevolgen van het incident hebben ondervonden of waarschijnlijk zullen ondervinden. Om het aantal getroffen gebruikers te berekenen, dient rekening te worden gehouden met het aantal getroffen natuurlijke personen of rechtspersonen, professionele klanten of eindklanten.

De duur van een incident dat invloed heeft op de beschikbaarheid van een dienst moet worden gemeten vanaf het moment waarop de correcte levering van die dienst wordt onderbroken tot het moment waarop deze weer is hersteld. Als een betrokken entiteit niet in staat is om vast te stellen wanneer de verstoring is begonnen, dient de duur van het incident te worden bepaald vanaf het moment dat het incident werd gedetecteerd of vanaf het moment dat het incident werd vastgesteld in de logboeken van het netwerk of systeem of in andere gegevensbronnen, waarbij de vroegste datum wordt weerhouden.

Er is bijvoorbeeld sprake van beperkte beschikbaarheid als een dienst van een betrokken entiteit aanzienlijk langzamer is dan de gemiddelde responstijd of als niet alle functionaliteiten van een dienst beschikbaar zijn. Waar mogelijk moeten objectieve criteria op basis van de gemiddelde responstijden van de door de betrokken entiteiten verleende diensten worden gebruikt om vertragingen in de responstijden te beoordelen. Voorbeelden van functionaliteiten zijn een chatfunctie of een zoekfunctie voor afbeeldingen.

3) Een gebeurtenis die financiële verliezen veroorzaakt of mogelijks zal veroorzaken

Een dergelijke gebeurtenis kan zich voordoen wanneer er sprake is van:

- een direct financieel verlies van meer dan €250 000 of een direct financieel verlies van 5% van de totale jaaromzet van de betrokken entiteit in het voorgaande volledige boekjaar, het laagste van de bedragen wordt in aanmerking genomen;
- het verlies of de verspreiding van intellectueel eigendom op een manier die de toekomstige opbrengsten of omzet in gevaar kan brengen;
- het onttrekken van bedrijfsgeheimen in de zin van artikel 2, lid 1, punt 1), van Richtlijn (EU) 2016/943 uit de betrokken entiteit.

Om de directe financiële verliezen als gevolg van een incident te bepalen, moeten de betrokken entiteiten rekening

houden met alle financiële verliezen die zij als gevolg van het incident hebben geleden, zoals:

- de kosten van de vervanging of de verplaatsing van software, hardware of infrastructuur;
- personeelskosten, inclusief de kosten van vervanging of verplaatsing van personeel, het aanwerven van extra personeel, het vergoeden van overuren en het herstellen van verloren of aangetaste vaardigheden en kennis;
- kosten in verband met het niet-nakomen van contractuele verplichtingen;
- reparatiekosten en schadevergoeding aan klanten, verliezen als gevolg van winstderving;
- interne en externe communicatiekosten;
- advieskosten, waaronder juridisch advies, forensische diensten en remediëringsdiensten;
- overige kosten in verband met het incident.

Administratieve boetes en de kosten voor de dagdagelijks bedrijfsvoering mogen echter niet worden beschouwd als financiële verliezen als gevolg van een incident. Deze omvatten onder andere:

- algemene onderhoudskosten voor infrastructuur, apparatuur, hardware en software;
- het op peil houden van de vaardigheden van het personeel;
- interne en externe kosten voor het verbeteren van het bedrijf na het incident, inclusief upgrades;
- verbeteringen en initiatieven op het gebied van risicobeoordeling;
- verzekeringspremies.

De betrokken entiteiten moeten de bedragen van de financiële verliezen bereken op basis van de beschikbare gegevens. Als de werkelijke bedragen van de financiële verliezen niet kunnen worden bepaald, moeten de entiteiten deze inschatten.

4) Een gebeurtenis die aanzienlijke materiële, lichamelijke of morele schade aan andere natuurlijke personen of rechtspersonen veroorzaakt of mogelijks kan veroorzaken

Een dergelijke gebeurtenis kan zich voordoen wanneer er sprake is van:

- gedeeltelijke of volledige vernietiging van fysieke of digitale activa;
- schade aan de fysieke infrastructuur waardoor de levering van producten of diensten langer duurt dan de contractueel gegarandeerde leveringstermijnen;
- schade zoals het overlijden van een persoon, ziekenhuisopname, letsels of invaliditeit;
- aanzienlijke financiële gevolgen.

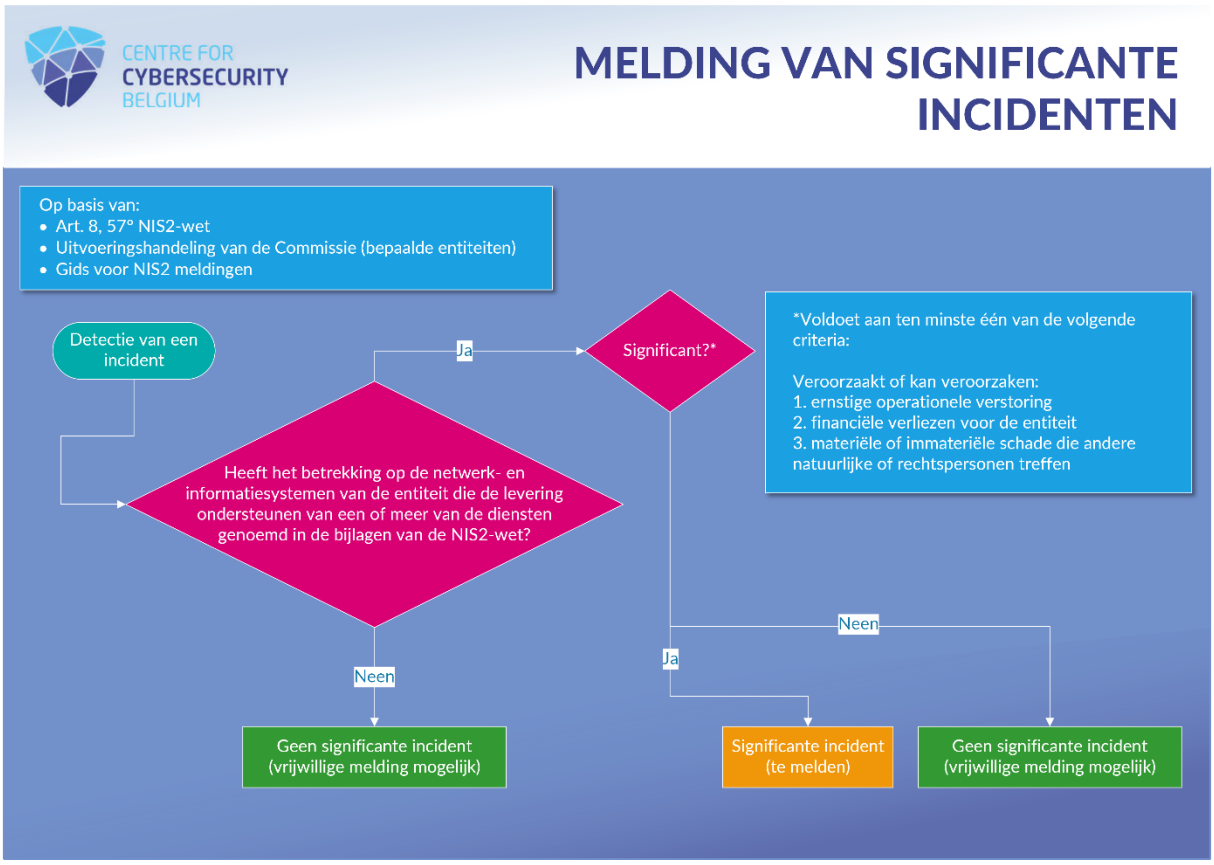
De betrokken entiteiten dienen ook incidenten te melden die de dood van natuurlijke personen of aanzienlijke schade aan hun gezondheid hebben veroorzaakt of zouden kunnen veroorzaken, aangezien dit bijzonder ernstige gevallen van aanzienlijke materiële of immateriële schade zijn. Een incident dat een betrokken entiteit treft, kan bijvoorbeeld resulteren in de onbeschikbaarheid van gezondheidszorg of hulpdiensten, of kan resulteren in het verlies van de vertrouwelijkheid of integriteit van gegevens.

Bij het bepalen of een incident aanzienlijke schade aan de gezondheid van een natuurlijke persoon heeft veroorzaakt of kan veroorzaken, moeten de betrokken entiteiten rekening houden met de vraag of het incident ernstige letsels of gezondheidsproblemen heeft veroorzaakt of mogelijks kan veroorzaken. Daartoe hoeven de betrokken entiteiten geen aanvullende informatie te verzamelen waartoe zij geen toegang hebben.

5) Een terugkerende gebeurtenis

Terugkerende incidenten die verband houden met dezelfde hoofdoorzaak en die afzonderlijk niet voldoen aan de criteria van een significant incident, moeten gezamenlijk worden beschouwd als een significant incident, als ze gezamenlijk voldoen aan de criteria van financiële verliezen (voor de entiteiten of voor derden) of de onbeschikbaarheid en de incidenten zich minstens twee keer hebben voorgedaan binnen een periode van 6 maanden.

Deze terugkerende incidenten kunnen aanzienlijke lacunes en tekortkomingen blootleggen in de risicobeheersprocedures voor cyberbeveiliging van de betrokken entiteit en haar maturiteitsniveau op het gebied van cyberbeveiliging. Bovendien kunnen deze terugkerende incidenten leiden tot aanzienlijke financiële verliezen voor de betrokken entiteit



A.3. ZIJN ER BIJZONDER REGELS?

De Europese Commissie zal in een uitvoeringshandeling (die binnenkort wordt aangenomen) de criteria specifiëren om te beoordelen of een incident als significant wordt beschouwd voor de volgende soorten entiteiten:

- DNS-dienstverleners;
- registers voor topleveldomeinnamen;
- aanbieders van cloudcomputingdiensten;
- aanbieders van datacentrumdiensten;
- aanbieders van netwerken voor de levering van inhoud;
- aanbieders van beheerde diensten;
- aanbieders van beheerde beveiligingsdiensten;
- aanbieders van onlinemarktplaatsen;
- aanbieders van onlinezoekmachines;
- aanbieders van platformen voor socialenetwerkdiensten;
- aanbieders van vertrouwensdiensten.

Entiteiten die onder de sectoren bankwezen en infrastructuur voor de financiële markt vallen in de zin van bijlage I van de NIS2-wet, en die onder het toepassingsgebied van verordening (EU) 2022/2554 van 14 december 2022 betreffende de digitale operationele weerbaarheid voor de financiële sector (DORA), met inbegrip van de activiteit van centrale effectenbewaarinstelling verricht door de Nationale Bank van België, zijn echter niet onderworpen aan de eerder aangehaalde meldingsprocedures.[1]

Verder gebruiken operatoren van elektronische communicatie die geïdentificeerd zijn als kritiek, de door het BIPT opgestelde escalatiematrix en passen zij de redundantiemiddelen toe waarin die matrix voorziet. Bovendien moeten de artikelen 34 en 35 van de NIS2-wet zo worden geïnterpreteerd dat een vroegtijdige waarschuwing zo snel mogelijk moet worden gegeven wanneer het onderliggende incident een invloed heeft op de noodoproepen zoals bedoeld in artikel 2, 60° van de wet van 13 juni 2005 betreffende de elektronische communicatie, gezien het belang

[1] Art. 6, § 3 van de NIS2-wet.

van die communicatie en de impact die de onbeschikbaarheid van die communicatie kan hebben op het leven of de fysieke integriteit van personen.

A.4. WANNEER MOET EEN SIGNIFICANT INCIDENT GEMELD WORDEN?

De meldingstermijnen gaan in op het moment dat de entiteit zich bewust wordt van een significant incident. De betrokken entiteit is daarom verplicht om incidenten te melden die, na haar eerste beoordeling, een ernstige operationele verstoring van diensten of financiële verliezen voor die entiteit kunnen veroorzaken, of andere natuurlijke of rechtspersonen kunnen treffen door aanzienlijk materiële of immateriële schade te veroorzaken.

Bijgevolg, als een betrokken entiteit een verdachte gebeurtenis heeft ontdekt, of nadat een derde (een persoon, een klant, een entiteit, een overheid, media of een andere bron) haar heeft gewezen op een potentieel incident, dient de betrokken entiteit de verdachte gebeurtenis tijdig te beoordelen, rekening houdend met de interne procedures, om te bepalen of het om een incident gaat, en zo ja, om de aard en de ernst van het incident vast te stellen. De betrokken entiteit moet daarom worden beschouwd als “zich bewust geworden” van het significante incident wanneer ze, na de eerste beoordeling, een redelijke mate van zekerheid heeft dat er zich een significant incident heeft voorgedaan.

Zodra een NIS2-entiteit redelijkerwijs weet dat ze te maken heeft met een significant incident, dient ze dit te melden aan het nationale CSIRT (het CCB). Deze melding verloopt in verschillende fasen[2]:

1) **Onverwijld en in elk geval binnen de 24 uur** nadat zij kennis hebben gekregen van het significant incident, bezorgt de entiteit een vroegtijdige waarschuwing (Early Warning);
2) **Onverwijld en in elk geval binnen 72 uur (24 uur voor verleners van vertrouwensdiensten) nadat zij kennis hebben gekregen van het significante incident,** bezorgt de entiteit een incidentmelding;
3) Op verzoek van het nationale CSIRT of van de eventuele betrokken sectorale overheid, bezorgt de entiteit een tussentijds verslag;
4) **Uiterlijk één maand na de in punt 2 bedoelde incidentmelding** stuurt de entiteit een eindverslag;
5) Als het eindverslag niet kan worden verstuurd omdat het incident nog aan de gang is, bezorgt de entiteit een voortgangsverslag en het eindverslag vervolgens binnen een maand na de definitieve afhandeling van het incident.

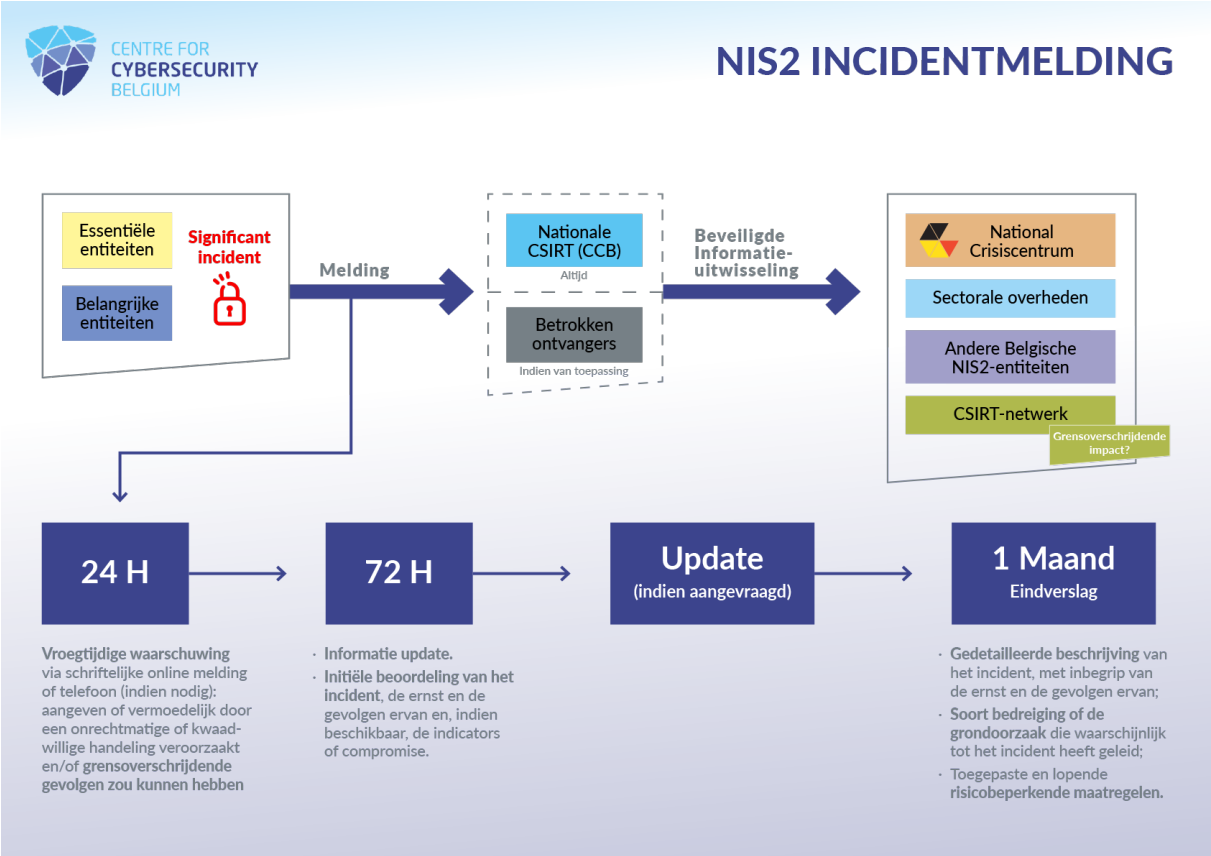
De term “onverwijld” betekent dat de entiteit die daartoe in staat is het incident zo snel mogelijk moet melden, zonder te wachten op de maximale termijnen van 24 uur en 72 uur. Alleen naar behoren gemotiveerde bijzondere omstandigheden kunnen ertoe leiden dat tot het einde van deze termijnen wordt gewacht. Het naleven van interne procedures van de organisatie, mag niet leiden tot een onredelijke vertraging bij het melden van het incident.

Als het waarschijnlijk is dat het ernstige incident gevolgen heeft voor de verlening van de in de bijlagen bij de wet vermelde diensten, dient de entiteit de ontvangers van haar diensten (voor zover zij identificeerbaar zijn) onverwijld op de hoogte te brengen. Aan deze informatieverplichting kan worden voldaan met elk beschikbaar middel (informatie op de website, mailinglijst, bericht in een applicatie, papieren communicatie, …)

De entiteit moet de ontvangers van haar diensten die mogelijks worden getroffen door een aanzienlijke cyberdreiging (zie de definitie hieronder in het gedeelte over vrijwillige kennisgeving) ook onverwijld in kennis stellen van alle maatregelen of correcties die deze ontvangers als reactie op deze dreiging kunnen toepassen.

Het CCB kan de informatie verkregen van de entiteiten delen met andere autoriteiten voor zover dat nodig is.

[2] Art. 35 NIS2-wet en onderstaand schema.



A.5. HOE MOET DE ENTITEIT EEN INCIDENT MELDEN?

Voor elk van de in het vorige punt genoemde fasen, wordt de melding gedaan door de betrokken entiteit via het online formulier op **https://notif.safeonweb.be** (tenzij onbeschikbaar of technisch onmogelijk). De verschillende velden van het online meldingsformulier worden toegelicht in bijlage 2 van deze gids.

Om belemmeringen met betrekking tot de melding te vermijden en gezien de vermoedelijke urgente situatie waarin de entiteit zich bevindt, is voor het gebruik van de melding geen voorafgaande authentificatie vereist.

Er is ook een telefoonnummer voor noodgevallen beschikbaar: (nr. +32 (0)2 501 05 60). Het doel van dit kanaal is entiteiten die dat wensen, in staat stellen in noodgevallen contact op te nemen met het nationale CSIRT wanneer onmiddellijke interventie door het nationale CSIRT vereist is bij een incident. Als het meldingsformulier onbeschikbaar is of als het voor de entiteit technisch onmogelijk is het formulier in te vullen, kan een dergelijk telefonisch contact in noodgevallen als gelijkwaardig worden beschouwd aan de melding bedoeld in artikel 35 van de NIS2-wet.

A.6. DE DOOR TE GEVEN INFORMATIE BIJ HET MELDEN VAN EEN SIGNIFICANT INCIDENT

In de verschillende stadia van de melding worden verschillende soorten informatie doorgegeven (zie het formulier op de website):

- **De vroegtijdige waarschuwing** (*Early warning*) geeft aan of het vermoeden bestaat dat het significante incident veroorzaakt is door een onrechtmatige of kwaadwillige handeling en of het al dan niet grensoverschrijdende gevolgen (d.w.z. een impact in een ander EU-land) kan hebben. Deze vroegtijdige waarschuwing bevat alleen de informatie die nodig is om het incident onder de aandacht van het CSIRT te brengen en stelt de betrokken entiteit in staat om zo nodig om bijstand te vragen.
  Een dergelijke waarschuwing mag de middelen van de meldende entiteit niet afleiden van activiteiten op het gebied van incidentenbeheer die prioriteit dienen te hebben, om te voorkomen dat de meldingsplicht

voor incidenten middelen afleidt van het beheer van significante incidenten of anderszins de inspanningen van de entiteit op dit gebied in gevaar brengt.

- Het doel van **de incidentmelding** binnen 72 uur is het actualiseren van de informatie die is gecommuniceerd als onderdeel van de vroegtijdige waarschuwing. Het biedt ook een eerste beoordeling van het incident, inclusief de ernst en de gevolgen ervan, evenals indicatoren van aantasting (IOC), indien beschikbaar.
  Net als bij vroegtijdige waarschuwing mag de incidentmelding geen beslag leggen op de middelen van de entiteit, om te voorkomen dat de meldingsplicht middelen afleidt van het beheer van significante incidenten of anderszins de inspanningen van de entiteit op dit gebied in gevaar brengt.
- **Het tussentijds verslag** bevat relevante updates over de situatie.
- **Het eindverslag** moet een gedetailleerde beschrijving van het incident bevatten, inclusief de ernst en de gevolgen ervan; het type bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid; de toegepaste en lopende risicobeperkende maatregelen; en in voorkomend geval, de grensoverschrijdende gevolgen van het incident.
- **Het voortgangsverslag** bevat zoveel mogelijk van de informatie die in het eindverslag zou moeten staan en die in het bezit is van de entiteit op het moment dat het voortgangsverslag wordt ingediend.

B. De vrijwillige meldingen

Essentiële en belangrijke entiteiten kunnen incidenten (niet-significante incidenten), cyberdreigingen en vermeden incidenten melden.

Een cyberdreiging is “elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden”.[3]

Een bijna-incident is “een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar had kunnen brengen, maar die met succes is voorkomen of zich niet heeft voorgedaan”.[4]

Ook entiteiten die geen essentiële of belangrijke entiteiten uitmaken, kunnen significante incidenten, cyberdreigingen en bijna-incidenten melden (ook al vallen ze niet onder het toepassingsgebied van de NIS2-wet).

Deze vrijwillige meldingen worden op dezelfde manier behandeld als verplichte meldingen. Het is echter mogelijk dat verplichte meldingen voorrang krijgen.

Een vrijwillige melding heeft niet als direct gevolg dat de meldende entiteit wordt geïnspecteerd of dat haar extra verplichtingen worden opgelegd waaraan zij niet zou zijn onderworpen als ze de melding niet had ingediend [5].

C. Vertrouwelijkheidsregels die van toepassing zijn op aangeleverde informatie in het kader van een melding

De NIS2-entiteit en haar toeleveranciers beperken de toegang tot informatie met betrekking tot incidenten, in de zin van de NIS2-wet, enkel tot de personen die deze informatie moeten kennen en er toegang to dienen te hebben om hun functies of taken met betrekking tot deze wet uit te voeren. Deze regel geldt ook voor het CCB (als nationaal CSIRT), het nationaal Crisiscentrum (NCCN) en eventueel bevoegde sectorale overheden.

Wanneer meldingen afkomstig zijn van een entiteit, worden deze onmiddellijk gedeeld door het nationale CSIRT met alle bevoegde sectorale autoriteiten en met het NCCN.[6]

---

[3] Art. 8, 10° NIS2-wet en art. 2, punt 8) van de verordening (EU) 2019/881 – « CSA ».
[4] Art. 8, 6° NIS2-wet.
[5] Art. 38, § 2, lid 3 NIS2-wet – onverminderd het voorkomen, opsporen, onderzoeken en vervolgen van strafbare feiten.
[6] Art. 34 NIS2-wet.

Informatie die door een NIS2-entiteit aan het CCB, het NCCN en de sectorale autoriteit wordt verstrekt, kan op anonieme wijze worden uitgewisseld in andere EU-lidstaten en met andere Belgische autoriteiten wanneer dit noodzakelijk is voor de toepassing van wettelijke bepalingen.

Deze overdracht van informatie is echter beperkt tot wat pertinent en evenredig is met het doel van de uitwisseling, in het kader van de Verordening EU 2016/679 (AVG), de vertrouwelijkheid van de betrokken informatie, de veiligheid en de commerciële belangen van de NIS2-entiteiten.

D. Wat gebeurt er indien een incident zich voordoet waar persoonsgegevens bij betrokken zijn?

Zoals nu reeds het geval is, vervangen meldingen van incidenten in het kader van NIS2 niet de meldingen in het geval van een inbreuk in verband met persoonsgegevens, bijvoorbeeld aan de Gegevensbeschermingsautoriteit (GBA). Er zullen nog steeds twee aparte meldingen nodig zijn.

De wet voorziet echter in een nauwe samenwerking tussen de nationale cyberbeveiligingsautoriteit en gegevensbeschermingsautoriteiten. Deze samenwerking zou kunnen leiden tot de ontwikkeling van gemeenschappelijke instrumenten.

Een melding aan de GBA gebeurt via hun website[7].

[7] https://www.gegevensbeschermingsautoriteit.be/professioneel/acties/datalek-van-persoonsgegevens.

Bijlage 1 - Overzichtstabel – Significant incident

Type gebeurtenis	Voorbeelden
Een vermoedelijk kwaadwillige gebeurtenis die de authenticiteit, integriteit, of vertrouwelijkheid van gegevens op de netwerk- en informatiesystemen van de entiteiten in gevaar brengt en die een ernstige operationele verstoring veroorzaakt of mogelijks zal veroorzaken.	• iemand heeft meer toegang verkregen dan voorzien, tot de netwerken, systemen of informatie ter ondersteuning van de levering van de dienst(en) van de entiteit; • een systeem of netwerk dat de levering van de dienst(en) van de entiteit ondersteunt, is of kan worden geconfigureerd door een persoon die niet de rechten zou mogen hebben om het systeem of netwerk van de entiteit te configureren; • een systeem of netwerk dat de levering van de dienst(en) van de entiteit ondersteunt, kan niet langer worden geconfigureerd door bevoorrechte gebruikers die de rechten zouden moeten hebben om het systeem of netwerk te configureren; • de configuraties of informatie van de systemen die de levering van de dienst(en) van de entiteit ondersteunen zijn onrechtmatig gewijzigd, verwijderd, toegevoegd of onbetrouwbaar gemaakt; • een systeem of netwerk dat de levering van de dienst(en) van de entiteit ondersteunt, voert taken uit die het niet hoort uit te voeren of voert taken niet uit die het hoort uit te voeren of voert taken niet uit die het hoort uit te voeren in verband met de toegang tot of de integriteit van het systeem of netwerk.
Een gebeurtenis die de beschikbaarheid van gegevens op de netwerk- en informatiesystemen van de entiteit in gevaar brengt en die een ernstige operationele verstoring veroorzaakt of mogelijks zal veroorzaken.	• minstens 20% van de gebruikers minstens één uur geen toegang heeft tot de dienst; • gebruikers minstens een uur lang geen toegang hebben tot de dienst en de entiteit het aantal getroffen gebruikers niet kan vaststellen (in relatieve of absolute zin); • de gebeurtenis een vertraging veroorzaakt in de levering van producten die de contractuele gegarandeerde levertijden overschrijdt; • met geplande onderhoudswerkzaamheden moet geen rekening worden gehouden (bijv. geplande uitschakeling voor onderhoud).
Financiële verliezen voor de betrokken entiteit	• een direct financieel verlies van meer dan €250.000 of een direct financieel verlies van 5% van de totale jaaromzet van de betreffende entiteit in het voorgaande volledige boekjaar, het laagste van de bedragen wordt in aanmerking genomen; • het verlies of de verspreiding van intellectueel eigendom op een manier die toekomstige opbrengsten of omzet in gevaar kan brengen; • de exfiltratie van bedrijfsgeheimen in de zin van artikel 2, lid 1, punt 1), van Richtlijn (EU) 2016/943 uit de betrokken entiteit.
Aanzienlijke materiële, lichamelijke of morele schade aan andere natuurlijke personen of rechtspersonen	• gedeeltelijke of volledige vernietiging van fysieke of digitale activa; • schade aan de fysieke infrastructuur waardoor de levering van producten langer duurt dan de contractueel gegarandeerde leveringstermijnen; • schade zoals overlijden van een persoon, ziekenhuisopname, letsels of invaliditeit; • aanzienlijke financiële gevolgen.
Een terugkerende gebeurtenis	

Bijlage 2 – Toelichting bij het aanmeldingsformulier

De verschillende velden in het meldingsformulier worden hieronder beschreven. De linkerkolom bevat de technische benaming van het veld (tussen vierkante haken) en de benaming die zichtbaar is voor gebruikers (in het vet). In de rechterkolom bevat de omschrijving van het veld. De velden zijn onderverdeeld in secties, elk met een eigen technische benaming (tussen vierkante haken en in hoofdletters).

[ENTITEIT DIE HET INCIDENT MELDT]	
[A. Field Name: 1-Submission_Type] **Gaat het over een incidentmelding die onder de NIS2-wet valt?**	In dit veld kunt u aangeven of uw melding onder de NIS2-wet valt (verplicht veld).
[B. Field Name : 2-Submitter] **Ik ben…**	In dit veld kunt u aangeven of u een NIS2-entiteit bent (verplicht veld).
[SPECIFIEKE NIS2 KENMERKEN]	
[C. Field Name: 3-NIS_Type] **Hoe wordt de organisatie in het kader van NIS2 gedefinieerd?**	In dit veld kunt u aangeven of u een belangrijke of essentiële entiteit bent in de zin van de NIS2-wet (verplicht veld).
[D. Field Name: 4-Sector] **In welke sector(en) is uw organisatie actief?**	In dit veld kunt u aangeven in welke sector(en) u actief bent, u kunt meer dan één vakje aankruisen (verplicht veld).
[E. Field Name: 5-NIS_Notification] **Welk type NIS2-incidentmelding dient u in?**	In dit veld kunt u aangeven in welke fase van de melding u zich bevindt. Pro memorie: de fasen worden beschreven in punt A. « Hoe snel moet een significant incident worden gemeld? » (verplicht veld).
[DETAILS VAN HET INCIDENT]	
[F. Field Name: 6-Malicious_Intent] **Denkt u dat dit incident het gevolg is van kwaad opzet?**	In dit veld kunt u aangeven of dit incident, volgens u, het gevolg is van kwaad opzet. Als u dit niet weet of er niet overtuigd van bent, kan u “onzeker” aanvinken (verplicht veld).
[G. Field Name: 7-Incident_Type] **Type Incident**	In dit veld kunt u uit een lijst het incidenttype of de incidenttypes kiezen die overeenkomen met het incident dat u wenst te melden. Het is mogelijk om meerdere vakjes aan te vinken (verplicht veld).
[H. Field Name: 8-Incident_Date] **Wanneer vond het incident plaats?**	In dit veld kunt u de datum invoeren in de indeling Maand/Dag/Jaar. In het geval van twijfel, kan het volgend veld (I.) worden gebruikt om alle informatie met betrekking tot wanneer het incident heeft plaatsgevonden te verstrekken) (optioneel veld).

[I. Field Name: 9-Incident_Description] **Beschrijf het incident (initiële oorzaak, impact op de organisatie, naam van het virus of de malware, getroffen gegevens en systemen, genomen maatregelen, betrokken besturingssystemen/software…)**	In dit veld kunt u de informatie vermelden die u in uw bezit hebt met betrekking tot het incident, inclusief aanwijzingen voor compromittering. Raadpleeg punt A. “Informatie die moet worden verstrekt bij de melding van een ernstig incident”, waarin wordt beschreven welke informatie in elke fase van de melding moet worden verstrekt, om te weten te komen welke informatie prioriteit moet krijgen. Het formulier bevat specifieke velden voor de oorzaken, gevolgen en ernst van het incident. Het veld heeft een maximum van 500 tekens (verplicht veld).
[J. Field Name: 9-Assessment_Severity] **Beoordeel de ernst van het incident**	In dit veld kunt u de ernst van het incident beschrijven. In het kader van vroegtijdige waarschuwing kan een dergelijke beoordeling zeer beknopt en/of gedeeltelijk zijn. Als onderdeel van de melding binnen 72 uur na het incident moet u een eerste beoordeling van de ernst van het incident geven. Als onderdeel van het eindrapport moet deze beoordeling gedetailleerd zijn. Het veld heeft een maximum van 500 tekens (verplicht veld).
[K. Field Name: 11-Assessment_Consequence] **Wat zijn de gevolgen van het incident?**	In dit veld kunt u de gevolgen van het incident beschrijven. In de context van een vroegtijdige waarschuwing kan een dergelijke beoordeling zeer beknopt en/of gedeeltelijk zijn. Als onderdeel van de incidentmelding binnen de 72 uur na het incident dient u een eerste beoordeling van de gevolgen van het incident te geven. Als onderdeel van het eindrapport dient deze beoordeling gedetailleerd te zijn. Hou er rekening mee dat het formulier specifieke velden bevat voor de potentiële grensoverschrijdende gevolgen van het incident. Het veld heeft een maximum van 500 tekens (verplicht veld).
[L. Field Name: 12-Threat_Type_Root_Cause] **Wat is de oorzaak van het incident?**	In dit veld kunt u aangeven of de oorzaak van het incident bekend is en zo ja, kunt u daarover informatie verstrekken. Houd er rekening mee dat u in het stadium van het eindrapport het type bedreiging of de hoofdoorzaak dient aan te geven die waarschijnlijk tot het incident heeft geleid. Het veld heeft een maximum van 500 tekens (verplicht veld).
[M. Field Name: 13-Cross_Border_Impact] **Denkt u dat dit incident kan leiden tot grensoverschrijdende gevolgen?**	In dit veld kunt u aangeven of u denkt dat het incident kan leiden tot grensoverschrijdende gevolgen. Indien u hier niet zeker over bent, vink dan “Onzeker” aan. Houd er rekening mee dat u in het stadium van het eindrapport, indien van toepassing, dient aan te geven wat de grensoverschrijdende gevolgen van het incident zijn (verplicht veld).
[N. Field Name: 14-Cross_Border_Impact_Description] **Gelieve details te geven over de potentiële grensoverschrijdende**	In dit veld kunt u details geven over de grensoverschrijdende impact van het incident. Houd er rekening mee dat dit veld enkel verschijnt indien u “ja“

gevolgen die dit incident kan veroorzaken:	heeft aangeduid in het vorige veld (M.) (optioneel veld)
[O. Field Name: 15-Police_Involved] **Hebt u het incident bij de politie gemeld? (als u het slachtoffer bent geworden van een geslaagde cyberaanval, raden wij u aan om aangifte te doen bij de politie)**	In dit veld kunt u aangeven of u het incident al bij de politie heeft gemeld. Het is raadzaam dit te doen in geval van een kwaadwillig of opzettelijk incident. (optioneel veld).
[P. Field Name: 16-Help_Needed] **Hebt u ondersteuning, onderzoek of advies nodig van het CCB?**	In dit veld kunt u, indien van toepassing, expliciet ondersteuning vragen van het CCB door het vakje 'ja' aan te vinken. Deze ondersteuning bestaat uit operationele begeleiding of advies over de uitvoering van mogelijke risicobeperkende maatregelen, of zelfs aanvullende technische ondersteuning (verplicht veld).
[Q. Field Name: 17-Help_Type_Needed] **Gelieve zo precies mogelijk aan te geven welke ondersteuning u nodig hebt van het CCB:**	In dit veld kunt u het type ondersteuning beschrijven dat u nodig hebt bij het beheer van het incident dat aanleiding gaf tot de melding. Deze ondersteuning bestaat uit operationele begeleiding of advies over de implementatie van mogelijke risicobeperkende maatregelen, of zelfs aanvullende technische ondersteuning. Het veld heeft een maximum van 500 tekens (verplicht veld).
[R. Field Name: 18-Actions_Taken] Welke **acties heeft u ondernomen?**	In dit veld kunt u de acties beschrijven die zijn ondernomen om het incident te beperken en/of te verhelpen. Houd er rekening mee dat dit een optioneel veld is, maar als onderdeel van het eindrapport moet u de genomen en lopende mitigerende maatregelen beschrijven. Het veld heeft een maximum van 500 tekens (verplicht veld).
[S. Field Name: 19-Resolved] **Is het incident nu opgelost?**	In dit veld kunt u aangeven of het incident is opgelost op het moment van de betreffende melding (verplicht veld).
[CONTACTGEGEVENS ENTITEIT]	
[T. Field Name: 20-Anonymous]	Dit veld is niet zichtbaar en geeft aan of de melding anoniem is gedaan.
[U. Field Name: 21-Contact_Person] **Contactpersoon**	In dit veld kunt u de naam van de contactpersoon voor incidentbeheer aangeven (optioneel veld).
[V. Field Name: 22-Organization] **Naam organisatie - KBO**	In dit veld kunt u de naam opgeven van de organisatie namens wie de melding wordt gedaan (verplicht veld).
[W. Field Name: 23-Email] **Email**	In dit veld kunt u het e-mailadres invoeren waarmee het CCB contact kan opnemen met de organisatie

	waarop het incident betrekking heeft (verplicht veld).
[X. Field Name: 24-Telephone] **Telefoonnummer**	In dit veld kunt u het telefoonnummer invoeren waarmee het CCB contact kan opnemen met de organisatie waarop het incident betrekking heeft (verplicht veld).
[Y. Field Name: 25-Location] **Waar vond het incident plaats?**	In dit veld kunt u de locatie aangeven waar het incident heeft plaatsgevonden (optioneel veld).

GIDS VOOR NIS2 MELDINGEN

Dit document wordt 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.

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-generaal
Wetstraat 18
1000 Brussel

Wettelijk depot:
D/2024/14828/010