FAQ NIS betreffende de aanbieders van essentiële diensten (AED's)

A. Identificatie

1) Wie zijn de verschillende bevoegde NIS-overheden in België voor aanbieders van essentiële diensten (AED's)?

1) Het Centrum voor Cybersecurity België (CCB) is de nationale overheid die belast is met de opvolging en coördinatie van de uitvoering van de wet van 7 april 2019 (NIS-wet), het nationale computer security incident response team (nationaal CSIRT) en het centraal nationaal contactpunt voor de betrekkingen op het niveau van de Europese Unie.

2) Het Nationaal Crisiscentrum van de FOD Binnenlandse Zaken (NCCN) is de overheid die, in samenwerking met het CCB, de identificatie van AED's coördineert.

3) De sectorale overheden:

- Voor Energie: **de federale Minister van Energie** of bij delegatie een leidend personeelslid van zijn/haar administratie.
- Voor Vervoer (met uitzondering van het vervoer over wateren toegankelijk voor zeeschepen): **de federale Minister van Mobiliteit** of bij delegatie een leidend personeelslid van zijn/haar administratie.
- Voor Vervoer over wateren toegankelijk voor zeeschepen: **de federale Minister bevoegd voor Maritieme Mobiliteit** of bij delegatie een leidend personeelslid van zijn/haar administratie.
- Voor Financiën, deelsector financiële instellingen: **de Nationale Bank van België** (NBB).
- Voor Financiën, deelsector financiële handelsplatformen: **de Autoriteit voor Financiële Diensten en Markten** (FSMA).
- Voor Gezondheidszorg: **de federale Minister van Volksgezondheid** (of bij delegatie een leidend personeelslid van zijn/haar administratie).
- Voor Digitale infrastructuren: **het Belgisch Instituut voor postdiensten en telecommunicatie** (BIPT).
- Voor Drinkwater: **het Nationaal Comité voor de beveiliging van de levering en distributie van drinkwater** (wordt momenteel opgericht).

2) Wat is een AED? Wat is een essentiële dienst?

De AED bedoeld in de NIS-wet is een publieke of private entiteit die daadwerkelijk een activiteit uitoefent in België die betrekking heeft op de verlening van een essentiële dienst in een van de sectoren opgenomen in bijlage I bij deze wet. Hij heeft minstens één vestiging op Belgisch grondgebied en is bij administratieve beslissing van de bevoegde sectorale overheid (zie vraag nr. 4 hierna) erkend als aanbieder van een ***essentiële dienst***.

Bijv.: het beheer van een transmissienet voor elektriciteit.

Om door de sectorale overheid als AED te worden aangewezen, moet de aanbieder aan vier cumulatieve criteria voldoen:

a) tot een van de sectoren of deelsectoren bedoeld in bijlage I bij de NIS-wet behoren:

Bijlage I bij de NIS-wet (sector, deelsector, soort AED)		
Sector	**Deelsector**	**Soort**
Energie 	a) Elektriciteit b) Aardolie c) Gas	Bijv.: distributienetbeheerders in de zin van artikel 2, 11°, van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt.
Vervoer 	a) Luchtvervoer b) Spoorvervoer c) Vervoer over water d) Vervoer over de weg	Bijv.: spoorwegondernemingen in de zin van artikel 3, 27°, van de Spoorcodex. Beheerders van havens in de zin van artikel 5, punt 7), van de wet van 5 februari 2007 betreffende de maritieme beveiliging.
Financiën 	a) Financiële instellingen b) Financiële handelsplatformen	Kredietinstellingen, centrale tegenpartijen, andere financiële instellingen Exploitanten van een financieel handelsplatform
Gezondheidszorg 	Zorginstellingen (waaronder ziekenhuizen en privé-klinieken)	Zorgverleners in de zin van artikel 3, punt g), van richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg.

Drinkwater 		Leveranciers en distributeurs van water bestemd voor menselijke consumptie.
Digitale infrastructuren 		Internetknooppunten (IXP) Leveranciers van DNS-diensten Registers van topleveldomeinnamen.

b) een dienst aanbieden die door de bevoegde sectorale overheid als "essentieel" wordt beschouwd;

c) de verlening van de dienst is afhankelijk van netwerk- en informatiesystemen (de NIS-wet gaat ervan uit dat dit het geval is);

d) een "incident" met betrekking tot de "beveiliging van netwerk- en informatiesystemen" van de aanbieder kan "aanzienlijke verstorende effecten" hebben voor de verlening van de essentiële dienst (volgens de criteria bepaald door de bevoegde sectorale overheid).

Een essentiële dienst is een dienst die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten. De bevoegde sectorale overheid bepaalt binnen haar sector de diensten die als "essentieel" worden beschouwd, met name rekening houdend met de essentiële diensten opgenomen in bijlage I bij de NIS-wet.

Bijv.: het beheer van een distributienet voor elektriciteit.

De drempelwaarden of weerslagniveaus voor de identificatie worden bepaald door de bevoegde sectorale overheid en houden minstens rekening met de volgende intersectorale criteria:

1. het aantal gebruikers dat afhankelijk is van de door de betrokken entiteit verleende dienst;
2. de afhankelijkheid van de andere in bijlage I bij de NIS-wet bedoelde sectoren van de door die entiteit verleende dienst;
3. de gevolgen die incidenten kunnen hebben, wat betreft mate en duur, voor economische of maatschappelijke activiteiten of voor de openbare veiligheid;
4. het marktaandeel van die entiteit;
5. de omvang van het geografische gebied dat door een incident kan worden getroffen;
6. het belang van de entiteit voor de instandhouding van een toereikend dienstverleningsniveau, rekening houdend met de beschikbare alternatieven voor het verlenen van die dienst.

3) Zijn overheden onderworpen aan de bepalingen van de NIS-wet?

De NIS-wet heeft zowel betrekking op private als op publieke entiteiten in ruime zin (administratieve overheden, overheidsbedrijven, instellingen van openbaar nut, intercommunales, enz.) die essentiële diensten aanbieden in België.

Momenteel is het toepassingsgebied van de NIS-wet beperkt tot publieke entiteiten die actief zijn in een van de sectoren opgenomen in bijlage I bij deze wet (bijvoorbeeld: gas- of elektriciteitsdistributie, drinkwaterdistributie, luchthavenbeheer, ziekenhuisbeheer, enz.) en die de bevoegde sectorale overheid heeft aangewezen als AED's. De huidige lijst van sectoren, deelsectoren en soorten AED's kan in de toekomst door de Koning worden uitgebreid.

Het spreekt vanzelf dat andere publieke entiteiten ook een ***essentiële dienst*** verlenen voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten, in het kader van hun taken van openbare dienst.

Los van de NIS-wet zijn deze publieke entiteiten al verplicht de wettelijke bepalingen na te leven die van toepassing zijn op hun netwerk- en informatiesysteem(systemen) (AVG Europese Verordening nr. 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, Verordening e-IDAS (EU) nr. 910/2014 van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties, de wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator, de aansprakelijkheidsregels van overheden, enz.).

4) Wat is het verschil tussen een AED en een exploitant van een kritieke infrastructuur (KI)?

Dit zijn twee verschillende begrippen die elkaar echter aanvullen.

Het begrip "kritieke infrastructuur" (KI) bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren verwijst naar een of meer specifieke elementen van een door een aanbieder verleende dienst die van essentieel belang zijn voor het behoud van vitale functies. Het betreft een installatie, een systeem of een deel daarvan.

Het begrip "essentiële dienst" bedoeld in de NIS-wet verwijst daarentegen naar de verlening van een dienst, in zijn geheel genomen (met alle componenten ervan), door een aanbieder die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten. Zo kan een AED ook de exploitant van een of meer kritieke infrastructuren zijn.

Verder is een nationale KI noodzakelijkerwijs gelegen in België, terwijl de installaties en systemen van een in België verleende essentiële dienst zich volledig of gedeeltelijk in het buitenland kunnen bevinden. Een Europese KI kan in België of in een andere lidstaat van de Europese Unie gelegen zijn.

De AED moet ook afhankelijk zijn van netwerk- en informatiesystemen om de goede werking van zijn essentiële diensten te waarborgen, terwijl dit niet noodzakelijk het geval is voor de exploitant van een KI (het toenemend gebruik van netwerk- en informatiesystemen door bedrijven en publieke entiteiten zorgt er evenwel voor dat dit onderscheid meer en meer theoretisch wordt).

Tot slot wordt een onderscheid gemaakt tussen de twee begrippen rekening houdend met de aard en de gevolgen van een eventueel incident. Een incident als bedoeld in de NIS-wet verwijst naar een gebeurtenis met een reële negatieve impact op de beveiliging van netwerk- en informatiesystemen, terwijl een incident als bedoeld in de wet van 1 juli 2011 verwijst naar een gebeurtenis die van dien aard is dat ze de veiligheid van de kritieke infrastructuur bedreigt, en dus niet noodzakelijk concrete gevolgen heeft voor de veiligheid van de infrastructuur of verband houdt met de beveiliging van de netwerk- en informatiesystemen van de infrastructuur.

Beide wetten gebruiken ook verschillende termen voor het potentiële incident waarmee het kritieke of essentiële karakter van de activiteiten van de aanbieder kan worden vastgesteld, namelijk de mogelijkheid van een incident dat aanzienlijke verstorende effecten kan hebben voor de verlening van een essentiële dienst voor de AED, of de mogelijkheid van de verstoring van de werking of de vernietiging van een installatie, een systeem of een deel daarvan die een aanzienlijke weerslag heeft doordat vitale maatschappelijke functies ontregeld raken. Beide begrippen delen niettemin de onderliggende wens om de continuïteit te waarborgen van activiteiten van openbaar belang die essentieel zijn voor de bevolking of de economie.

5) Hoe wordt een AED aangewezen?

De bevoegde sectorale overheid gaat na welke aanbieders in haar sector actief zijn, en wijst de AED's aan bij administratieve beslissing, op basis van de weerslagniveaus of drempelwaarden voor de identificatie. Het Centrum voor Cybersecurity België (CCB) en het Nationaal Crisiscentrum (NCCN) nemen deel aan het voorafgaand overleg over de aanwijzing en, in voorkomend geval, ook de betrokken gewestelijke of gemeenschapsoverheden.

Een ***intersectoraal criterium*** is een factor die gemeenschappelijk is voor alle sectoren bedoeld in bijlage I bij de NIS-wet en die het belang van een ***verstorend effect*** bepaalt (het aantal gebruikers, de afhankelijkheid van de andere sectoren, de gevolgen van een incident, het marktaandeel, het geografische gebied dat door een incident kan worden getroffen, het belang van de entiteit voor de instandhouding van een toereikend dienstverleningsniveau).

Een ***sectoraal criterium*** is een factor die eigen is aan een sector of deelsector bedoeld in bijlage I bij de NIS-wet en die het belang van een ***verstorend effect*** bepaalt.

Omdat de drempelwaarden en weerslagniveaus die door de sectorale overheden worden gekozen gevoelig zijn voor de openbare veiligheid, worden ze niet openbaar gemaakt (de bestuursdocumenten betreffende de identificatieprocedure worden beschouwd als bestuursdocumenten die verband houden met de veiligheid van de bevolking, de openbare orde en de veiligheid, in de zin van artikel 6, § 1, van de wet van 11 april 1994 betreffende de openbaarheid van bestuur, en die niet het voorwerp mogen uitmaken van inzake, uitleg of mededeling in afschrift voor het publiek).

De sectorale overheid moet, behoudens uitzondering (de NIS-wet gaat ervan uit dat de exploitatie van een kritieke infrastructuur afhankelijk is van netwerk- en informatiesystemen), alle exploitanten van kritieke infrastructuren (als bedoeld in de wet van 1 juli 2011) in haar sector aanwijzen als AED's.

Bijv.: de beheerder van een transmissienet voor elektriciteit die werd geïdentificeerd als exploitant van een nationale KI wordt in principe ook aangewezen als AED.

Omgekeerd wordt een aangewezen AED niet automatisch geïdentificeerd als exploitant van een of meer KI's: dat hangt af van de locatie van zijn installaties, uitrustingen en systemen (al dan niet in België) en van het kritieke belang ervan (in geval van vernietiging of verstoring van de werking ervan).

De sectorale overheid moet de lijst van AED's van haar sector regelmatig bijwerken (minstens om de twee jaar).

6) Welke verplichtingen zijn van toepassing op AED's?

AED's hebben verschillende soorten verplichtingen:

- maatregelen nemen voor de beveiliging van de netwerk- en informatiesystemen die verband houden met de verlening van hun essentiële dienst(en);
- melden van beveiligingsincidenten bij de netwerk- en informatiesystemen die verband houden met de verlening van hun essentiële dienst(en);
- toezien op de beveiliging van de netwerk- en informatiesystemen die verband houden met de verlening van hun essentiële dienst(en): interne en externe audit;
- samenwerken en informatie uitwisselen met de verschillende bevoegde NIS-overheden.

B. Beveiligingsmaatregelen

7) Welke maatregelen voor de beveiliging van netwerk- en informatiesystemen (NIS) zijn van toepassing op een AED?

7.1 Algemene beveiligingsmaatregelen

De AED moet technische en organisatorische maatregelen nemen:

a) die passend en evenredig zijn

• Op adequate en gepaste wijze reageren op een gegeven situatie (de maatregelen hierop afstemmen)**.**

b) om de risico's voor de beveiliging van netwerk- en informatiesystemen te beheersen (na een risicoanalyse)

- **Risico**: "elke redelijkerwijs vast te stellen omstandigheid of gebeurtenis met een mogelijke negatieve impact op de beveiliging van netwerk- en informatiesystemen" (art. 6, 15°, van de NIS-wet)
- **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" (art. 6, 9°, van de NIS-wet).

- **Beschikbaarheid**: vermogen van een systeem om toegankelijk en bruikbaar te zijn → de werking ervan waarborgen
- **Authenticiteit**: vermogen van een systeem om te bevestigen dat het is wat het beweert te zijn
- **Integriteit**: vermogen van een systeem om niet te worden gewijzigd door niet-gemachtigde entiteiten
- **Vertrouwelijkheid**: vermogen van een systeem om toegang tot de gegevens ervan door niet-gemachtigde personen te voorkomen.

- **Netwerk- en informatiesysteem** (art. 6, 8°, van de NIS-wet):

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.

c) om te zorgen voor een niveau van fysieke en logische beveiliging

- Ervoor zorgen dat een systeem met een bepaalde mate van betrouwbaarheid bestand is tegen gebeurtenissen die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van de verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via dat systeem worden aangeboden of toegankelijk zijn, in gevaar kunnen brengen.

- **Fysiek:** maatregelen die de weerbaarheid van de materiële elementen van de netwerk- en informatiesystemen waarborgen (fysieke toegang tot informatica-uitrusting, serverlokaal, enz.).
- **Logisch:** maatregelen die de weerbaarheid van de logische elementen van de netwerk- en informatiesystemen waarborgen (toegangscontrole voor software, encryptie, monitoring, antivirus, enz.).

d) afgestemd op de risico's die zich voordoen rekening houdend met de huidige stand van de technische kennis

- De techniek moet op de markt aanwezig zijn als een product dat reeds wordt verkocht, niet als prototype waardoor ze moeilijk beschikbaar zou zijn.
- *Technology watch* is absoluut noodzakelijk

e) passend om incidenten die de beveiliging van de netwerk- en informatiesystemen aantasten, te voorkomen

- Passend: hangt af van het voorwerp waarop ze betrekking hebben en of ze afgestemd zijn op het voorkomen van incidenten
- Incidenten voorkomen: de gevolgen ervan minimaliseren, om de continuïteit van de verlening van de essentiële diensten te waarborgen.

De AED moet een ***beveiligingsbeleid*** (I.B.B.) uitwerken en toepassen ***voor de netwerk- en informatiesystemen*** waarvan de essentiële diensten die hij verleent afhankelijk zijn. Dit I.B.B. bevat minstens de geïmplementeerde concrete beveiligingsdoelstellingen en -maatregelen.

7.2 Specifieke maatregelen

De Koning kan, bij koninklijk besluit, bepaalde specifieke beveiligingsmaatregelen opleggen aan alle AED's (of aan bepaalde soorten AED's) van een of meer sectoren (of deelsectoren).

Ook de bevoegde sectorale overheid kan, bij individuele administratieve beslissing, specifieke beveiligingsmaatregelen opleggen aan een bepaalde AED.

8) Hoe kan een AED bewijzen dat hij de beveiligingsverplichtingen naleeft?

De AED kan zelf aan de externe auditinstelling en/of inspectiedienst bewijzen dat hij de algemene en specifieke beveiligingsverplichtingen naleeft (art. 20 en 21 van de NIS-wet) door zijn risicoanalyse, het beveiligingsniveau van zijn technische/organisatorische maatregelen, de geschiktheid van de maatregelen om incidenten te voorkomen enz. adequaat te documenteren. In dat geval berust de bewijslast voor de conformiteit bij de AED.

De AED kan ook een ISO 27001 certificaat (niet verplicht) gebruiken dat wordt uitgereikt door een instelling voor de conformiteitsbeoordeling die geaccrediteerd is door BELAC (of door een gelijkwaardige Europese instelling) en dat betrekking heeft op de maatregelen voor de beveiliging van de netwerk- en informatiesystemen die noodzakelijk zijn voor de verlening van de essentiële dienst of diensten. In dat geval geniet de AED het vermoeden dat zijn IBB conform de beveiligingseisen is, wanneer voldaan is aan de eisen van de norm ISO/IEC 27001 “Managementsystemen voor informatiebeveiliging” (of aan een nationale, buitenlandse of internationale norm die door de Koning als gelijkwaardig wordt erkend).

De naleving van de norm ISO/IEC 27001 houdt immers in dat de wettelijke eisen die van toepassing zijn op de AED worden gerespecteerd (met inbegrip van de *algemene* beveiligings*maatregelen* die voortvloeien uit de NIS-wet en de *specifieke* beveiligings*maatregelen*).

Dit vermoeden geldt tot het bewijs van het tegendeel door de inspectiedienst. De bewijslast berust dus bij de inspectiedienst en niet bij de AED.

9) Wat zijn de eerste stappen die een AED moet nemen om zich in regel te stellen?

Binnen 3 maanden na zijn aanwijzing moet de AED:

- de sectorale overheid een beschrijving bezorgen van de netwerk- en informatiesystemen waarvan de verlening van de betrokken essentiële dienst of diensten afhankelijk is;
- een intern ***contactpunt voor de beveiliging van netwerk- en informatiesystemen*** aanwijzen;
- de contactgegevens van het contactpunt bezorgen aan de bevoegde sectorale overheid.

Binnen een termijn van 12 maanden na zijn aanwijzing moet de AED zijn ***beveiligingsbeleid voor zijn netwerk- en informatiesystemen*** (I.B.B.) uitwerken.

Binnen 3 maanden na de uitwerking van zijn I.B.B. voert de AED zijn eerste ***interne audit*** uit.
Binnen een termijn van 24 maanden na zijn aanwijzing moet de AED de in zijn ***I.B.B.*** beschreven maatregelen implementeren.

Binnen 24 maanden na de uitvoering van zijn eerste ***interne audit*** voert de AED zijn eerste ***externe audit*** uit.

C. Melding van incidenten

10) Welke gebeurtenissen moeten verplicht door een AED worden gemeld?

a) Een AED (die niet onder het toezicht van de Nationale Bank van België "NBB" staat) moet **alle incidenten** melden **die gevolgen hebben** voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit (*) van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn.

Volgens art. 24, § 1, van de NIS-wet moeten alle incidenten die aanzienlijke gevolgen hebben voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de netwerk- en informatiesystemen waarvan de door de aanbieder verleende essentiële dienst of diensten afhankelijk zijn, onverwijld worden gemeld. Art. 24, § 3, bepaalt echter dat, indien geen weerslagniveaus en/of drempelwaarden als bedoeld in paragraaf 2 zijn bepaald, de aanbieder alle incidenten meldt die gevolgen hebben voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn.

(*) zie definities vraag 7.

De NIS-wet voorziet in de mogelijkheid om, bij koninklijk besluit, weerslagniveaus en/of drempelwaarden voor de melding van incidenten te bepalen, of nog, verschillende meldingscategorieën volgens de mate van impact van het incident. Tot nu toe werden echter nog geen dergelijke koninklijke besluiten aangenomen.

b) Een AED die onder het toezicht van de NBB staat, meldt **alle incidenten die aanzienlijke gevolgen hebben** voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn.

De NBB is ermee belast deze aanzienlijke gevolgen te bepalen.

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

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.

11) Binnen welke termijn moet een NIS-incident worden gemeld?

De AED moet het incident onverwijld melden, dat wil zeggen zo vlug mogelijk.

De AED moet niet wachten tot hij over alle relevante informatie over een incident beschikt om het te melden. Zodra de AED over de informatie beschikt die nodig is om de gevolgen van het incident volledig of gedeeltelijk te beoordelen, moet hij het melden.

12) Aan wie moet de AED een NIS-incident melden?

a) De AED (die niet onder het toezicht van de NBB staat) moet het incident tegelijk aan drie overheden melden:

- het Centrum voor Cybersecurity België (CCB);
- het Nationaal Crisiscentrum (NCCN);
- de sectorale overheid en/of haar sectorale CSIRT.

In de praktijk gebeurt deze gelijktijdige melding in één stap via het NIS-meldingsplatform.

b) De AED die onder het toezicht van de NBB staat, moet het incident enkel melden aan de NBB, volgens de door die laatste vastgestelde modaliteiten.

Indien de NBB de AED verplicht om het meldingsplatform te gebruiken, wordt het incident ook tegelijk aan het CCB en het NCCN gemeld. Indien de NBB het gebruik van het meldingsplatform niet oplegt, bezorgt zij de melding zelf onverwijld aan het CCB en het NCCN.

Deze uitzondering vloeit voort uit het feit dat sommige financiële instellingen al onderworpen zijn aan sectorale meldingsverplichtingen op Europees niveau tegenover de Europese Centrale Bank.

13) Hoe moet de AED een NIS-incident melden?

Een AED (die niet onder het toezicht van de NBB staat) moet het incident melden via ***het NIS-meldingsplatform***: https://nis-incident.be/nl/.

Het platform is toegankelijk via internet door middel van een beveiligde verbinding en een voor elke AED unieke identificatiesleutel (login/gebruikersnaam en wachtwoord).

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

Meer informatie over de melding van een incident vindt u in de Gids voor de melding door AED's op de website van het CCB [URL].

14) Welke informatie moet de AED bezorgen bij de melding van een NIS-incident?

De AED moet het formulier voor het melden van incidenten gebruiken dat door het CCB ter beschikking wordt gesteld op het NIS-meldingsplatform: ***https://nis-incident.be***.

Het meldingsformulier omvat alle beschikbare informatie die toelaat de aard, de oorzaken, de effecten en de gevolgen van het incident te bepalen:

a) de naam en contactgegevens van de aanbieder en de door hem verleende 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.

15) Welke vertrouwelijkheidsregels zijn van toepassing op de informatie die bij een NIS-incident wordt bezorgd?

De AED en zijn onderaannemers beperken de toegang tot de informatie over incidenten, in de zin van de NIS-wet, 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.

Deze regel geldt ook voor het CCB (nationaal CSIRT), het NCCN, de sectorale overheid en het eventuele sectorale CSIRT.

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

De informatie die een AED aan het CCB, het NCCN en de sectorale overheid bezorgt, mag worden uitgewisseld met autoriteiten van andere lidstaten van de Europese Unie en met andere Belgische 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, met inachtneming van Verordening EU 2016/679, de vertrouwelijkheid van de betrokken informatie, alsook van de veiligheid en de commerciële belangen van de AED.

16) Wat zijn de verschillende meldingsfasen bij een NIS-incident?

De meldingsprocedure kan verschillende fasen omvatten:

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

b) ***Bijkomende meldingen*** moeten regelmatig worden verstuurd of zodra de AED over nieuwe informatie beschikt. Doel van deze bijkomende meldingen is het CCB, de sectorale overheid of haar sectorale CSIRT, en het NCCN op de hoogte te houden van de status van het incident. De

AED doet dan een nieuwe melding op het platform, waarbij hij enkel de nieuwe gegevens en het referentienummer van de initiële melding vermeldt.

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

De AED moet het CCB en de sectorale overheid, of in voorkomend geval het sectorale CSIRT, op de hoogte houden van de evolutie van het incident en de ondernomen remediërende acties.

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

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

Op verzoek van het CCB, het NCCN, de sectorale overheid of haar sectorale CSIRT meldt de AED via het meldingsplatform een actualisering van het meldingsformulier (“eindverslag”) waarin hij de behandeling van het incident beschrijft vanaf het ontdekken tot het afsluiten ervan en alle informatie van het meldingsformulier overneemt.

Bijkomende meldingen (bedoeld in artikel 8, § 3, van het NIS-KB) door een AED in geval van nieuwe informatie of belangrijke ontwikkelingen betreffende het incident verlopen via het meldingsplatform.

17) Welke andere verplichtingen heeft de AED in geval van een NIS-incident?

De AED die getroffen is door een incident, is verplicht het incident aan te pakken en reactieve maatregelen te nemen om het op te lossen. Hij blijft verantwoordelijk voor de aanpak van het incident.

De AED moet incidenten of verdachte gebeurtenissen onderzoeken die hem door het CCB, de sectorale overheid of het NCCN worden gemeld.

Het CCB, de sectorale overheid of haar sectorale CSIRT, en het NCCN kunnen de AED bijkomende informatie vragen over diens meldingen.

AED’s die onder het toezicht van de NBB staan, behandelen het incident rekening houdend met de wettelijke bepalingen en voorschriften die op hen toepasselijk zijn gemaakt door de NBB en/of de Europese Centrale Bank.

Wanneer de omstandigheden dit toelaten, verstrekt het CCB de AED die de melding heeft ingediend, 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.

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

Naargelang de ingevoerde informatie wordt de AED met een standaardbericht ingelicht over zijn verplichting om eventuele inbreuken in verband met persoonsgegevens te melden aan een van de

"toezichthoudende autoriteiten" met behulp van de geschikte meldingstools (bijvoorbeeld: www.gegevensbeschermingsautoriteit.be/meldformulier-voor-gegevenslekken).

Bijzondere regels betreffende persoonsgegevens

Voor de verwerking van persoonsgegevens door een AED 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.

De AED moet de gegevens (met inbegrip van de persoonsgegevens) niet langer bewaren 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.

19) Welke gebeurtenissen mogen op vrijwillige basis worden gemeld door een potentiële AED?

"Potentiële aanbieders van essentiële diensten" (publieke of private entiteiten die in België actief zijn in een van de sectoren opgenomen in bijlage I bij de NIS-wet: Energie, Vervoer, Financiën, Gezondheidszorg, Drinkwater en Digitale infrastructuren, maar niet zijn aangewezen als AED's) mogen op vrijwillige basis incidenten melden die aanzienlijke gevolgen hebben voor de continuïteit van de door hen verleende diensten.

Bijv.: een nieuwe aanbieder die actief is in een van de sectoren opgenomen in bijlage I bij de NIS-wet en die nog niet is aangewezen als AED, of een aanbieder die actief is in een van deze sectoren maar die zich onder de door de sectorale overheid bepaalde drempelwaarden of weerslagniveaus voor de aanwijzing bevindt.

Deze vrijwillige melding mag er niet toe leiden dat de meldende entiteit verplichtingen worden opgelegd waaraan zij niet onderworpen zou zijn als zij die melding niet had gedaan.

Bij de behandeling van meldingen mogen het CCB, de sectorale overheid of haar sectorale CSIRT, en het NCCN de door de NIS-wet opgelegde verplichte meldingen prioritair verwerken ten opzichte van vrijwillige meldingen.

Vrijwillige meldingen worden enkel verwerkt wanneer die verwerking geen onevenredige of overmatige belasting vormt voor voornoemde overheden.

Vrijwillige meldingen worden rechtstreeks naar het CCB gestuurd door de potentiële AED volgens de modaliteiten vermeld op de website van het Centrum voor Cybersecurity België (dienst CERT.be): https://cert.be/nl/een-incident-melden-form.

D. Controle

20) Hoe worden AED's gecontroleerd?

Er zijn drie soorten controles van de AED's vastgelegd:

a) een **interne controle** (interne audit);

b) een **externe controle** (externe audit) **door een *geaccrediteerde of erkende instelling voor de conformiteitsbeoordeling***;

c) een **externe controle** (inspectie) **door de leden van de bevoegde sectorale inspectiedienst.**

a) interne controle

De AED moet minstens eenmaal per jaar en op zijn kosten een **interne audit** uitvoeren (door leden van zijn personeel en/of externe consultants) van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële diensten afhankelijk zijn. Deze interne audit moet de AED toelaten zich ervan te vergewissen dat de in zijn I.B.B. bepaalde technische en organisatorische maatregelen goed worden toegepast en regelmatig worden gecontroleerd.

De AED bezorgt zijn interne auditverslagen binnen dertig dagen aan de bevoegde sectorale overheid.

b) externe controle

De AED laat, minstens om de drie jaar en op zijn kosten, een **externe audit** uitvoeren door een instelling voor de conformiteitsbeoordeling die geaccrediteerd is door BELAC (of door een gelijkwaardige accreditatieautoriteit van een andere lidstaat van de Europese Unie die de erkenningsakkoorden van de "European Cooperation for Accreditation" medeondertekend heeft) of die eventueel erkend is door de sectorale overheid.

De lijst van geaccrediteerde of erkende instellingen voor de conformiteitsbeoordeling is beschikbaar bij de sectorale overheid die ze actueel houdt.

De AED bezorgt zijn externe auditverslagen (eventueel samen met zijn opmerkingen) binnen dertig dagen aan de bevoegde sectorale overheid.

c) inspectie

De inspectiediensten kunnen op elk ogenblik controles uitvoeren op de naleving door de AED van de beveiligingsmaatregelen en de regels voor het melden van incidenten.

Het CCB of de sectorale overheid kan de inspectiedienst aanbevelen om een inspectie uit te voeren.

De inspectiedienst kan een beroep doen op experten.

21) Sancties

AED's die de verplichtingen van de NIS-wet niet naleven, kunnen worden veroordeeld tot strafrechtelijke sancties door een strafrechter (strafrechtelijke geldboetes en gevangenisstraffen) of tot administratieve sancties door de administratieve overheden (administratieve geldboetes).

	Strafrechtelijke sanctie (per inbreuk) In geval van herhaling van dezelfde feiten binnen een termijn van drie jaar wordt de geldboete verdubbeld en de overtreder bestraft met een gevangenisstraf van 15 dagen tot 3 jaar.	**Administratieve sanctie** (per inbreuk) In geval van herhaling van dezelfde feiten binnen een termijn van drie jaar wordt de administratieve geldboete verdubbeld.
Alle nuttige informatie aan de NIS-overheden bezorgen die daarom verzoeken.	Gevangenisstraf van 8 dagen tot 1 jaar en strafrechtelijke geldboete van 208 € (26 € x 8 (*)) tot 400.000 € (50.000 € x 8 (*)) of een van deze twee straffen.	Geldboete van 500 tot 125.000 €
Technische en organisatorische maatregelen nemen voor de beveiliging van de netwerk- en informatiesystemen waarvan de verleende diensten afhankelijk zijn.	Gevangenisstraf van 8 dagen tot 1 jaar en geldboete van 208 € (26 € x 8 (*)) tot 240.000 € (30.000 € x 8 (*)) of een van deze twee straffen.	Geldboete van 500 tot 100.000 €
Incidenten melden die de beveiliging aantasten van de netwerk- en informatiesystemen waarvan de verleende diensten afhankelijk zijn.	Gevangenisstraf van 8 dagen tot 1 jaar en geldboete van 208 € (26 € x 8 (*)) tot 160.000 € (20.000 € x 8 (*)) of een van deze twee straffen.	Geldboete van 500 tot 75.000 €
De vertrouwelijkheid/het beroepsgeheim waarborgen van de in het kader van de NIS-wet verwerkte informatie.	Gevangenisstraf van 1 jaar tot 3 jaar en geldboete van 800 € (100 € x 8 (*)) tot 8.000 € (1.000 x 8 (*)) of een van deze twee	

+ onderaannemers	straffen (zie art. 458 van het Strafwetboek).	
Jaarlijks een interne audit van de netwerk- en informatiesystemen **uitvoeren.** **Om de drie jaar een externe audit** van de netwerk- en informatiesystemen **laten uitvoeren** (door een geaccrediteerde of erkende instelling).	Gevangenisstraf van 8 dagen tot 1 jaar en geldboete van 208 € (26 € x 8 (*)) tot 400.000 € (50.000 x 8 (*)) of een van deze twee straffen.	Geldboete van 500 tot 200.000 €
Opzettelijke belemmering van de uitvoering van een controle door een lid van de inspectiedienst, **weigering** om informatie mee te delen die naar aanleiding van een controle wordt gevraagd, of opzettelijke mededeling van foutieve of onvolledige informatie.	Gevangenisstraf van 8 dagen tot 2 jaar en geldboete van 208 € (26 € x 8 (*)) tot 600.000 € (75.000 € x 8 (*)) of een van deze twee straffen.	Geldboete van 500 tot 200.000 €
Iedere handeling waarbij een persoon die optreedt voor rekening van een AED **nadelige gevolgen ondervindt** bij de uitvoering, te goeder trouw en in het kader van zijn functie, van de verplichtingen die voortvloeien uit de NIS-wet.		

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

22) Moet de AED nog een klacht indienen in verband met de gemelde NIS-incidenten?

Indien de AED het slachtoffer is van een inbreuk inzake cybercriminaliteit en een klacht wenst in te dienen, moet hij dit zelf doen. De melding van een NIS-incident houdt op zich geen indiening van een strafklacht in.

De AED wordt echter sterk aangeraden een strafklacht in te dienen om de kans op herhaling te beperken.

Tot slot, overeenkomstig artikel 29 van het Wetboek van Strafvordering kunnen ambtenaren die bij AED's werken alsook ambtenaren van de verschillende overheden die meldingen ontvangen, verplicht

zijn om strafrechtelijke inbreuken te melden waarvan zij op de hoogte zijn bij de uitoefening van hun functie, en alle informatie daarover aan het openbaar ministerie te bezorgen.

E. 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 (afgekort "NIS-wet") (bekendgemaakt in het Belgisch Staatsblad en in werking getreden op 3 mei 2019).

-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 (afgekort "NIS-KB") (bekendgemaakt in het Belgisch Staatsblad en in werking getreden op 18 juli 2019).

-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 ("NIS-richtlijn").

-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").

-Artikel 36/47 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België (*B.S.*, 28 maart 1998, blz. 9377 e.v.).