CENTRE FOR CYBER SECURITY BELGIUM

Verplichte melding van een incident door een AED (samenvatting)			
Wat?	**Aan wie?**	**Binnen welke termijn?**	**Hoe?**
a) voor AEDs, <u>die niet onder het toezicht van de Nationale Bank van België "NBB" staat</u> : **<u>Alle incidenten die gevolgen hebben</u>** voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn. **b)** Voor AED **<u>die onder het toezicht van de NBB staat</u>**, Alle incidenten die **<u>aanzienlijke gevolgen</u>** 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.	**a) voor AEDs, <u>die niet onder het toezicht van de Nationale Bank van België "NBB" staat</u>, gelijktijdige melding van het incident aan drie autoriteiten :** 1. Het Centrum voor Cybersecurity België (CCB); 2. Het Nationaal Crisiscentrum (NCCN); 3. De sectorale overheid en/of haar sectorale CSIRT. **b) voor AED's <u>die onder het toezicht van de Nationale Bank van België</u>**: rechtstreekse melding aan de Nationale Bank van België (NBB), volgens de door die laatste vastgestelde modaliteiten.	Het incident moet **onverwijld** worden gemeld, 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. Wanneer hij uit de informatie waarover hij beschikt kan afleiden dat het incident verplicht gemeld moet worden, moet hij dit onverwijld doen.	**a) voor AEDs, <u>die niet onder het toezicht van de Nationale Bank van België "NBB" staat</u>:** het formulier op het NIS-meldingsplatform invullen: <u>https://nis-incident.be</u> De informatie wordt dan via het platform automatisch naar de verschillende betrokken autoriteiten gestuurd. Het platform is toegankelijk via internet door middel van een beveiligde verbinding en een voor elke aanbieder van essentiële diensten unieke identificatiesleutel. Indien het NIS-meldingsplatform niet beschikbaar is, moet de AED het incident melden volgens de modaliteiten vermeld op de website van het CCB (<u>https://cert.be/nl/een-incident-melden-form</u>). **b) voor AED's die onder het toezicht van de Nationale Bank van België:** rechtstreekse melding aan de Nationale Bank van België (NBB), volgens de modaliteiten vastgesteld door de NBB. 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.

Definities:

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.

De beschikbaarheid is het vermogen van een informatiesysteem om toegankelijk en bruikbaar te zijn op verzoek van een gemachtigde entiteit. Het is de bedoeling om de normale werking van een informatiesysteem te waarborgen.

De vertrouwelijkheid is het vermogen van een informatiesysteem om toegang tot de gegevens ervan door niet-gemachtigde personen of entiteiten te voorkomen. Het is de bedoeling te vermijden dat de informatie in verkeerde handen valt of openbaar wordt gemaakt zonder toestemming van de verantwoordelijke van het informatiesysteem.

De integriteit is het vermogen van een informatiesysteem om niet te worden gewijzigd door niet-gemachtigde entiteiten. Het is de bedoeling zich te beschermen tegen een onwettige en schadelijke wijziging van het informatiesysteem.

De authenticiteit is het vermogen van een informatiesysteem om te bevestigen dat het is wat het beweert te zijn. Het is de bedoeling zeker te zijn dat de gegevens afkomstig zijn van een welbepaald informatiesysteem.

Andere verplichtingen:

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.**

De aanbieder van essentiële diensten blijft verantwoordelijk voor de aanpak van het incident.

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

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:

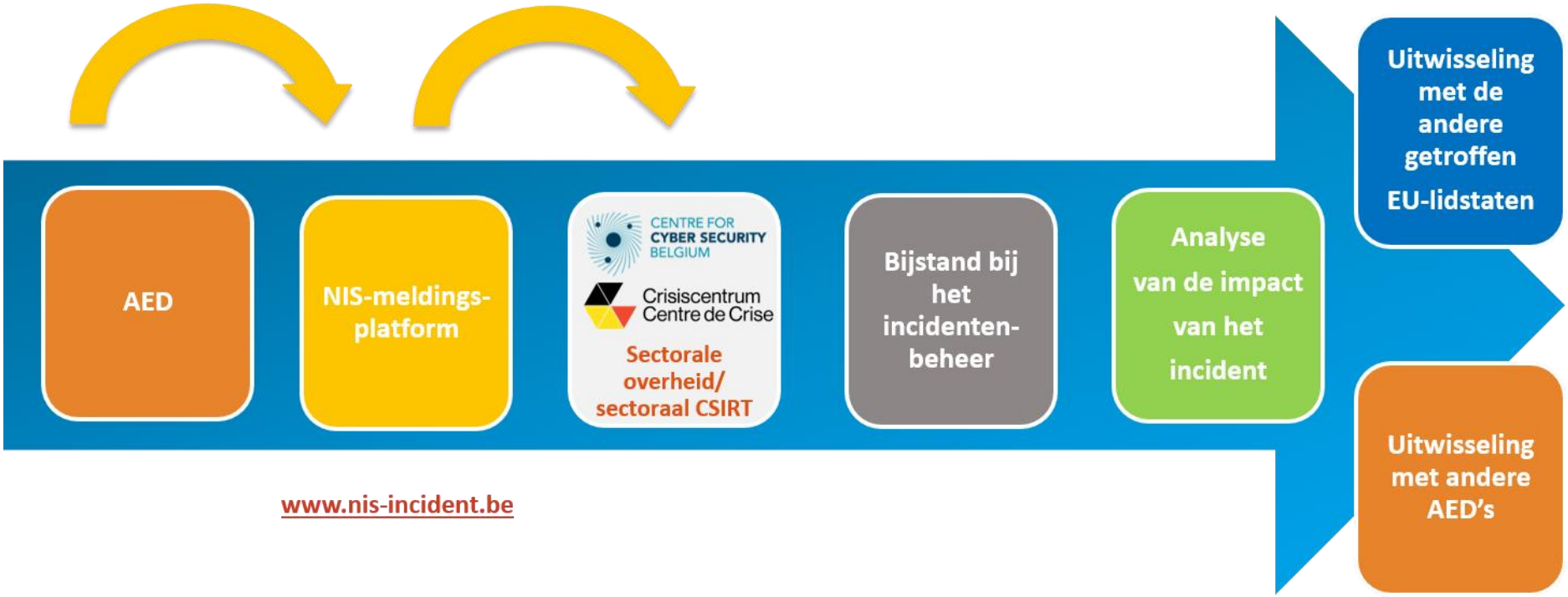
- via e-mail: cert@cert.be
- telefonisch: +32 (0)2 501 05 60

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

Melding van NIS-incidenten
(behalve AED's onder het toezicht van de NBB)



www.nis-incident.be


EUROPEAN CENTRAL BANK
EUROSYSTEM
CSIRTs NETWORK
NIS COOPERATION GROUP
Melding van NIS-incidenten
AED's onder het toezicht van de NBB
AED
National Bank OF BELGIUM
NIS-meldings-platform
Crisiscentrum Centre de Crise
CENTRE FOR CYBER SECURITY BELGIUM
Bijstand bij het incidenten-beheer
Analyse van de impact van het incident
Uitwisseling met de andere getroffen EU-lidstaten
Uitwisseling met andere AED's
www.nis-incident.be

Vrijwillige melding			
Wat?	**Aan wie?**	**Binnen welke termijn?**	**Hoe?**
Alle incidenten die aanzienlijke gevolgen hebben voor de continuïteit van een essentiële dienst. 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.	Aan het CCB.	Zo vlug mogelijk	Volgens de modaliteiten vermeld op de website van het Centrum voor Cybersecurity België (dienst CERT.be): https://cert.be/nl/een-incident-melden-form