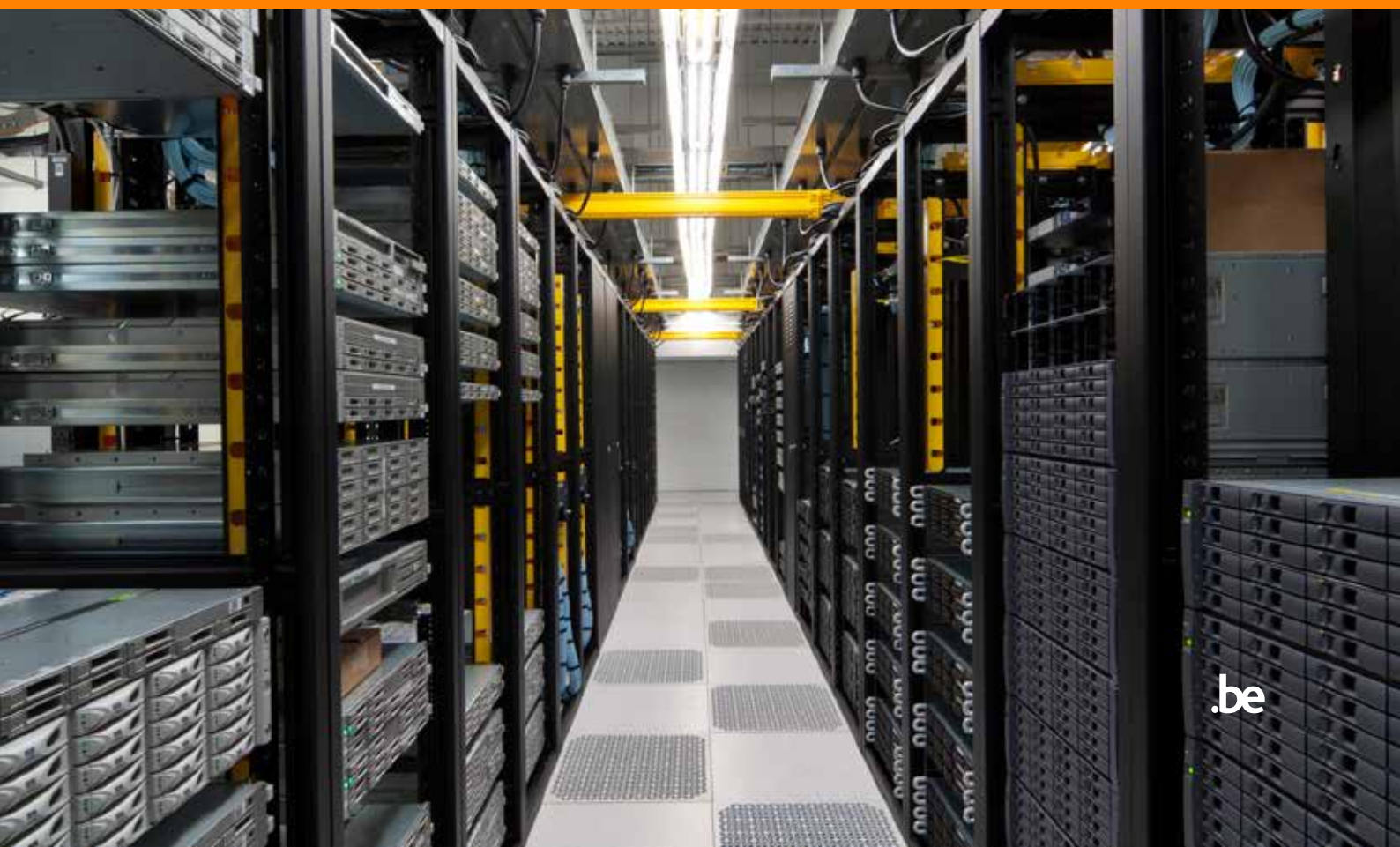
CENTRE FOR
CYBER SECURITY
BELGIUM

CHANCELLERY OF
THE PRIME MINISTER

CENTRUM VOOR CYBER SECURITY BELGIUM

/ JAARVERSLAG 2015



VOORWOORD

2015 was een zeer belangrijk jaar voor het Centrum voor Cybersecurity België (CCB) , het was het jaar van haar oprichting.

Met het Koninklijk Besluit van 10/10/2014 werd het CCB op papier opgericht. Het duurde echter tot augustus 2015 eer het CCB effectief van start kon met het uitoefenen van haar taken. In augustus 2015 werden immers de Directeur, Miguel De Bruycker, en de Adjunct-Directrice, Phédra Clouner, voor een mandaat van 5 jaar benoemd.

De bij Koninklijk Besluit opgelegde taken zijn ambitieus en omvangrijk: als nationale autoriteit heeft het CCB de opdrachten om het Belgische beleid ter zake op te volgen, te coördineren en toe te zien op de uitvoering ervan. Daarnaast zal ze vanuit een geïntegreerde en gecentraliseerde aanpak de verschillende projecten op het vlak van cyberveiligheid beheren, de coördinatie verzekeren tussen de betrokken diensten en de publieke overheden en de private of wetenschappelijke sector. Het CCB moet voorstellen formuleren tot aanpassing van het regelgevend kader op het vlak van cyberveiligheid en het crisisbeheer in samenwerking met het Coördinatie- en Crisiscentrum bij cyberincidenten verzekeren.

Hier stopt het echter niet: bij de taken van het CCB horen ook het opstellen, verspreiden en toezien op de uitvoering van standaarden, richtlijnen en veiligheidsnormen voor de verschillende informatiesystemen van de administraties en publieke instellingen, het coördineren van de Belgische vertegenwoordiging in internationale fora voor cyberveiligheid, de opvolging van internationale verplichtingen en voorstellen van het nationale standpunt op dit vlak. Tenslotte zal het CCB ook de evaluatie en certificatie van de veiligheid van informatie- en communicatiesystemen coördineren en eindgebruikers informeren en sensibiliseren over informatie- en communicatiesystemen.

Om dit tot een goed einde te brengen werd een strategisch plan opgesteld. Dit plan zal als leidraad voor de werking van het CCB voor de komende 5 jaar dienen. In het strategisch plan worden prioriteiten aangeduid, doelstellingen opgesomd en een tijdskader uitgetekend voor de opstart van projecten. Drie grote fasen worden geïdentificeerd: een start-up fase van 6 maanden (oktober 2015-maart 2016) gevolgd door een build-up fase met een horizon van 3 jaar en tenslotte een maturiteitsfase met een horizon van 5 jaar. Voor elk van de drie fasen wordt een afzonderlijk operationeel plan opgesteld, goedgekeurd en bijgestuurd waar nodig. Ook de doelstellingen voor deze fasen werden in het strategisch plan geformuleerd.

Voor de opstartfase werd bepaald dat het CCB personeel zal aanwerven en zich zal focussen op de organisatie van eigen middelen. Het CCB zal ook een overzicht maken van de bestaande cybercapaciteiten in België en een nationale incidentprocedure bij cyberaanvallen opstellen, in nauwe samenwerking met het Coördinatie- en Crisiscentrum.

Internationaal worden eerste contacten gelegd met buurlanden Frankrijk, Luxemburg en Nederland, met het oog op een nauwe samenwerking naar de toekomst toe. Het nationale Computer Emergency Response Team (CERT) wordt onder het bestuur van het CCB geplaatst en eventuele overlappingen van verantwoordelijkheden bij overheidsdiensten worden weggewerkt.

Tijdens de daaropvolgende build-up fase worden projecten opgestart en opgevolgd. In de maturiteitsfase tenslotte tracht het CCB over alle bouwstenen te beschikken om de strategische objectieven te behalen.

In dit rapport blikken we terug op de opstartfase van het CCB. Zeven van de tien beoogde medewerkers werden gerekruteerd.

Een officiële rondvraag naar bestaande cyberveiligheidscapaciteiten in België werd uitgestuurd naar cyberbetrokken diensten. Zo kunnen we de huidige capaciteiten in België juist in kaart brengen.
In december 2015 startte het CCB samen met alle betrokken diensten met de opstelling van een Belgisch nationaal cybernoodplan. Dit noodplan heeft als voornaamste doelstelling het organiseren van een antwoordstructuur op de cybersecurity crisissen en incidenten die een coördinatie of beheer op nationaal niveau vereisen.

Ook werden de eerste contacten met buitenlandse cybercentra gelegd. We stelden het CCB voor aan het Nationaal Cyber Security Centrum (NCSC) in Nederland, het Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) in Frankrijk en het govCERT in Luxemburg, om een nauwere samenwerking naar de toekomst toe te bespreken.

We werpen ten slotte ook een korte blik naar de volgende fase, de build-up fase. Verder in dit rapport komt de lezer namelijk meer te weten over toekomstige geplande projecten die het CCB wenst op te starten. Nu de rekrutering van het personeel bijna rond is, staan vele projecten voor de build-up fase reeds in de steigers. Met de planning van deze projecten zal het CCB niet enkel beantwoorden aan de taken die haar werden opgelegd bij Koninklijk Besluit, ze zullen tevens bijdragen aan het behalen van de doelstelling die het CCB voor zichzelf heeft bepaald: tegen 2020 wordt België een digital safe haven voor burgers en bedrijven.

Veel leesplezier!

Miguel De Bruycker

01

INTERVIEW

01

HET CENTRUM VOOR CYBERSECURITY BELGIË IS OPGERICHT BIJ KONINKLIJK BESLUIT VAN 10 OKTOBER 2014 TOT OPRICHTING VAN HET CENTRUM VOOR CYBERSECURITY BELGIË. OP 10 AUGUSTUS 2015 WERDEN MIGUEL DE BRUYCKER TOT DIRECTEUR EN PHÉDRA CLOUNER TOT ADJUNCT DIRECTRICE BENOEMD. IN DIT INTERVIEW BLIKKEN DE KERSVERSE DIRECTEURS TERUG OP DE EERSTE ZES MAANDEN VAN DE OPRICHTING VAN HET CENTRUM.

EERST EN VOORAL: PROFICIAT MET JULLIE BENOEMING! EEN NIEUW CENTRUM OPRICHTEN EN LEIDEN IS EEN ZWARE TAAK DIE OP JULLIE SCHOUDERS VIEL. WAT GING DOOR JULLIE HEEN NA DE BENOEMING VOOR DIT AMBITIEUZE PROJECT ?

Miguel: Ik was ten eerste zeer blij om aan deze ambitieuze taak te beginnen. Cyberveiligheid is een ontzettend boeiend domein en ik ben dan ook vereerd te kunnen werken aan een cyberveiliger België.

Phédra: Het is ontzettend spannend een volledig nieuw centrum te mogen oprichten. Ik besefte dat het geen makkelijke taak zou worden, maar ik was en ben nog steeds heel gemotiveerd om dit tot het beste einde te brengen. Cyberveiligheid is inderdaad een breed domein en een die steeds verandert. Bovendien zal het belang van cyberveiligheid enkel toenemen, het is dus zeker onze taak om snel te kunnen anticiperen.

DE EERSTE TWEE MAANDEN BESTOND HET CENTRUM VOOR CYBERSECURITY BELGIË UIT JULLIE BEIDEN.

- **Kenden jullie elkaar reeds voordien ?**
  Phédra: de cyberwereld in België is niet zo groot, ik ben Miguel al enkele keren tegengekomen op cyberveiligheidsconferenties.
- **Hoe is de onderlinge samenwerking verlopen ?**
  Miguel: zeer goed! Een van onze eerste taken was het samen opstellen van het strategisch plan. We hebben een ambitieus strategisch plan opgesteld en laten goedkeuren door de ministerraad. Deze samenwerking tussen ons beiden is uitstekend verlopen!

DE EERSTE TAAK WAS HET STARTEN VAN REKRUTERINGEN OM HET TEAM TE VERVOLLEDIGEN. IS DIT ONDERTUSSEN REEDS GELUKT ?

Miguel: 7 van de 10 beoogde medewerkers zijn gerekruteerd. In oktober 2015 verwelkomden we onze communicatieverantwoordelijke, in februari 2016 een projectleider en een juridisch adviseur. In maart 2016 tenslotte heeft de tweede projectleider het team vervoegd en enkele weken later een medewerker die de academische samenwerking zal coördineren. De wervingsprocedure voor twee office managers is ook reeds achter de rug. In juni verwelkomen we een Franstalige en een Nederlandstalige office manager.

Later dit jaar starten we nog met de rekrutering van een projectleider die best practices en whitepapers zal opstellen en verspreiden naar de bedrijfswereld.

HET CCB IS NIET DE ENIGE IN HAAR SOORT. IN ANDERE EUROPESE LANDEN BESTAAN REEDS LANGER NATIONALE CENTRA VOOR CYBERSECURITY.

- **Loopt België achter ten opzichte van haar buurlanden wat cybersecurity betreft ?**
  Miguel: Het klopt dat nationale centra voor cybersecurity reeds langer bestaan in onze buurlanden. Zeggen dat België hierdoor achter staat is nogal kort door de bocht. Bij verschillende overheidsdiensten zoals bijvoorbeeld de politie, het leger, justitie en het crisiscentrum bestaan reeds langer cyberafdelingen die een doeltreffend beleid voeren. Ook het CERT.be, het Cyber Emergency Response Team, bestaat al langer. Het CCB zal daarom ook in samenwerking met deze verschillende diensten acties ondernemen. Bestaande capaciteiten worden optimaal benut, en projecten zullen op elkaar worden afgestemd.

IN HET KONINKLIJK BESLUIT TER OPRICHTING VAN HET CCB LEZEN WE DAT OOK INTERNATIONALE SAMENWERKING HOOG OP DE AGENDA STAAT. HOE ZAL HET CENTRUM VOOR CYBERSECURITY BELGIË SAMENWERKEN MET BUITENLANDSE CYBERCENTRA ?

Phédra: Miguel en ik zijn het CCB gaan voorstellen bij het Nationaal Cyber Security Centrum (NCSC) in Nederland, het Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) in Frankrijk en het govCERT in Luxemburg. Onze uitdrukkelijke wens om nauwer samen te werken binnen de Benelux en met Frankrijk werd besproken. Deze werkbezoeken waren trouwens voor de interne organisatie zeer belangrijk. Aangezien zij reeds langer bestaan kunnen we leren uit hun oprichtingsparcours en de keuzes die zij hierbij maakten.

OP 26 OKTOBER WERD HET STRATEGISCH PLAN VAN HET CCB DOOR DE EERSTE MINISTER VOORGESTELD AAN DE PERS. HOE BLIKKEN JULLIE HIER OP TERUG?

Miguel: Een heel belangrijke dag! We waren enerzijds blij dat ons strategisch plan werd voorgesteld aan het grote publiek, anderzijds betekende dit dat we een officiële 'go' hadden gekregen om te beginnen met de verwezenlijking van onze ambitieuze plannen.

Phédra: ik was best wel nerveus en benieuwd naar de reacties op het strategische plan. Deze bleken over het algemeen zeer positief!

IN DECEMBER VERVOEGDE U DE RAAD VAN BESTUUR VAN DE CYBER SECURITY COALITION BELGIUM. WELKE ROL ZAL HET CCB SPELEN IN DEZE COALITIE ?

Miguel: Publiek-private samenwerking is zeer belangrijk, ook in de cyberwereld. Cyberveiligheid is immers een gedeelde verantwoordelijkheid. We trachten zoveel mogelijk partners aan tafel te krijgen om samen stappen te ondernemen naar een beleid bij organisaties die aandacht heeft voor cyberveiligheid. De vertrouwensrelatie die binnen de Coalitie wordt opgebouwd, concurrenten zitten nota bene samen aan tafel om oplossingen te delen voor cyberveiligheidsproblemen, vind ik persoonlijk ook heel mooi. Het is enkel samen dat we een front kunnen vormen tegen cybercriminaliteit.

Van september 2015 tot maart 2016 werd het CCB opgestart. Het CCB was gedurende deze fase maar beperkt operationeel en werkte in eerste instantie rond de realisatie en de organisatie van de eigen middelen.

WAT WAS DE GROOTSTE REALISATIE VAN HET CCB TIJDENS DE OPSTARTFASE?

Miguel: In april 2016 hebben we een eerste versie van het cybernoodplan voorgelegd aan alle partners die

01

betrokken zijn. De reacties zijn overwegend positief en we verwachten dan ook dat dit plan snel operationeel wordt.

Phédra: ook de rekrutering van het CCB-personeel is goed verlopen. Dankzij de uitstekende hulp die we kregen vanuit de Kanselarij zijn de selecties en aanwervingen bijna tot een goed einde gebracht. Een gemotiveerd team is immers cruciaal om de vele taken die het CCB heeft tot een goed einde te brengen.

EEN VAN DE DOELSTELLINGEN VAN DE OPSTARTFASE WAS HET IN KAART BRENGEN VAN HET ACTUELE BELGISCHE CYBER SECURITY LANDSCHAP. HOE HEBBEN JULLIE DIT AANGEPAKT?

Miguel: In oktober 2015 hebben we een brief gestuurd naar alle betrokken diensten in België met de vraag ons hun huidige capaciteiten in cyberveiligheid kenbaar te maken. Met deze informatie hebben we een duidelijk beeld gekregen van de actuele capaciteiten in België, zodat we een gericht beleid kunnen voeren naar de toekomst toe.

NA DE OPSTARTFASE (6MAANDEN) VOORZIET HET CCB EEN BUILD-UP FASE MET EEN HORIZON VAN 3 JAAR. WAT ZIJN DE UITDAGINGEN VOOR DE KOMENDE 3 JAAR ?

Phédra: In de build-up fase zullen we de bouwstenen creëren om de uiteindelijke doelstelling van het CCB, tegen 2020 van België een cyber safe haven te maken voor organisaties en bedrijven, te volbrengen. Deze bouwstenen zijn meer concreet de projecten die onze projectleiders opstarten en begeleiden.

Hartelijk bedankt voor dit interview en veel succes met jullie opdracht!
(Andries Bomans)

HET CENTRUM VOOR CYBERSECURITY BELGIË EN HAAR MEDEWERKERS

Van links naar rechts: **Andries Bomans:** communicatieverantwoordelijke
Jo De Muynck: projectleider
Nathalie Van Raemdonck: beleidsmedewerker academische samenwerking
Valéry Vander Geeten: juridisch adviseur
Phédra Clouner: adjunct-directrice
Miguel De Bruycker: directeur
Philippe Moisse: projectleider

02

CYBER SECURITY COALITION

02

SINDS 2015 BRENGT DE CYBER SECURITY COALITION VERTEGENWOORDIGERS VAN DE OVERHEIDSSECTOR, DE PRIVÉSECTOR EN DE ACADEMISCHE WERELD SAMEN IN ÉÉN ORGANISATIE. DIE BENADERING IS UNIEK IN BELGIË EN ZORGT ERVOOR DAT ERVARING, BEST PRACTICES, OPPORTUNITIES EN THREATS KUNNEN WORDEN UITGEWISSELD EN DAT EEN BEWUSTMAKINGSBELEID INZAKE CYBERSECURITY KAN WORDEN UITGEWERKT.

DE COALITIE HEEFT HAAR BIJDRAGE AAN HET BELGISCHE CYBERVEILIGHEIDSBELEID REEDS BEWEZEN:

- **uitwisseling van ervaring en kennis tussen cybersecuritydeskundigen sinds 2015.**
- **nationale bewustmakingscampagne in samenwerking met CERT.be voor het gebruik van wachtzinnen in plaats van wachtwoorden. Deze nationale campagne werd ondersteund door de website www.safeonweb.be en was erg succesvol.**
- **publicatie van de "cyber security incident management guide ". Een gids die een volledige en pragmatische benadering biedt van de manier waarop er in organisaties met cyberincidenten moet worden omgegaan.**
- **het tot stand brengen van een daadwerkelijke samenwerking met het Centrum voor Cybersecurity België.**

Miguel De Bruycker werd als directeur van het Centrum voor Cybersecurity België op 7 december 2015 lid van de raad van bestuur van de Coalitie. De Cyber Security Coalition heeft in samenwerking met het Centrum voor Cybersecurity België de "cyber security incident management guide " opgesteld.

In 2016 zal de Coalition op vier niveaus verder blijven werken:

- **bewustmaking, essentieel op het gebied van cybersecurity;**
- **uitwisseling van kennis;**
- **inter-CSIRT-samenwerking;**
- **aanbevelingen en policies.**

Het CCB zal in elk van deze 4 domeinen haar bijdrage leveren en de Coalition in haar geheel steunen.

03

PLATFORM CYBER SECURITY

03

BIJ KB (2/06/2015) WERD IN JUNI 2015 HET STRATEGISCH COMITÉ EN HET COÖRDINATIECOMITÉ VOOR INLICHTING EN VEILIGHEID (CCIV) OPGERICHT. BEIDE ORGANEN MOETEN DE GECOÖRDINEERDE UITVOERING VAN DE BESLISSINGEN VAN DE NATIONALE VEILIGHEIDSRAAD VERZEKEREN.

HET STRATEGISCH COMITÉ IS ERMEE BELAST ELK VOORSTEL TE ONDERZOEKEN IN HET KADER VAN HET DOOR DE NATIONALE VEILIGHEIDSRAAD TE BEPALEN INLICHTINGEN- EN VEILIGHEIDSBELEID. HET COÖRDINATIECOMITÉ WORDT ERMEE BELAST OM AAN DE NATIONALE VEILIGHEIDSRAAD GECOÖRDINEERDE VOORSTELLEN VOOR TE LEGGEN AANGAANDE :

- **het algemeen inlichtingen- en veiligheidsbeleid,**
- **de coördinatie van de strijd tegen de financiering van het terrorisme en van de verspreiding van massavernietigingswapens, en**
- **het beleid inzake de bescherming van gevoelige informatie.**

Het moet eveneens actieplannen ontwikkelen voor elke door de Nationale Veiligheidsraad bepaalde prioriteit en deze opvolgen of nieuwe prioriteiten voorstellen, de efficiënte samenwerking en uitwisseling van informatie tussen de inlichtingen- en veiligheidsdiensten bevorderen en de gecoördineerde uitvoering van de beslissingen van de Nationale Veiligheidsraad verzekeren. De leden van het Coördinatiecomité Inlichting en Veiligheid zijn allemaal leidinggevenden van de diensten en overheden die betrokken zijn bij het inlichtingen- en veiligheidsbeleid.

Het CCIV telt acht permanente leden. Deze zijn de administrateur-generaal van de Staatsveiligheid, de chef van de Algemene Dienst Inlichting en Veiligheid van het leger, de directeur van het OCAD, de commissaris-generaal van de federale politie, de directeur-generaal van de Algemene Directie Crisiscentrum van Binnenlandse Zaken, de voorzitter van het directiecomité van de FOD Buitenlandse Zaken (of een vertegenwoordiger), een lid van het College van procureurs-generaal en de federale procureur.

Zes leden zetelen enkel voor dossiers die hen aanbelangen: de administrateur-generaal van de Algemene Administratie van Douane en Accijnzen, de directeur van het Centrum voor Cybersecurity België, de voorzitter van de Cel voor Financiële Informatieverwerking, de directeur-generaal van het Directoraat-generaal Luchtvaart, de directeur-generaal van het Directoraat-generaal Maritiem Vervoer en de voorzitter van de Nationale Veiligheidsoverheid.

De Directeur van het Centrum voor Cybersecurity België is een niet-permanent lid en zetelt dus enkel in het CCIV bij cyber-gerelateerde dossiers.

Het Coördinatiecomité voor Inlichting en Veiligheid heeft een aantal platformen gecreëerd waaronder twee voor Cyber: het platform Cyber Security en het onderplatform Cyber Intelligence.

Het CCB is de piloot van het platform Cyber Security en neemt de organisatie en coördinatie voor haar rekening. Ze bepaalt ook de agenda in overleg met de permanente leden van dit platform.
Het doel van dit platform is om in samenspraak met de betrokken overheidsdiensten te komen tot een nationaal Cyber Security beleid waarin deze diensten een gepaste inspanning leveren en samen tot een geïntegreerde Belgische cyber security capaciteit komen. Door het optimaliseren van de informatie-uitwisseling zullen de bevolking, de bedrijven, de overheid en de vitale sectoren zich gepast kunnen beschermen.

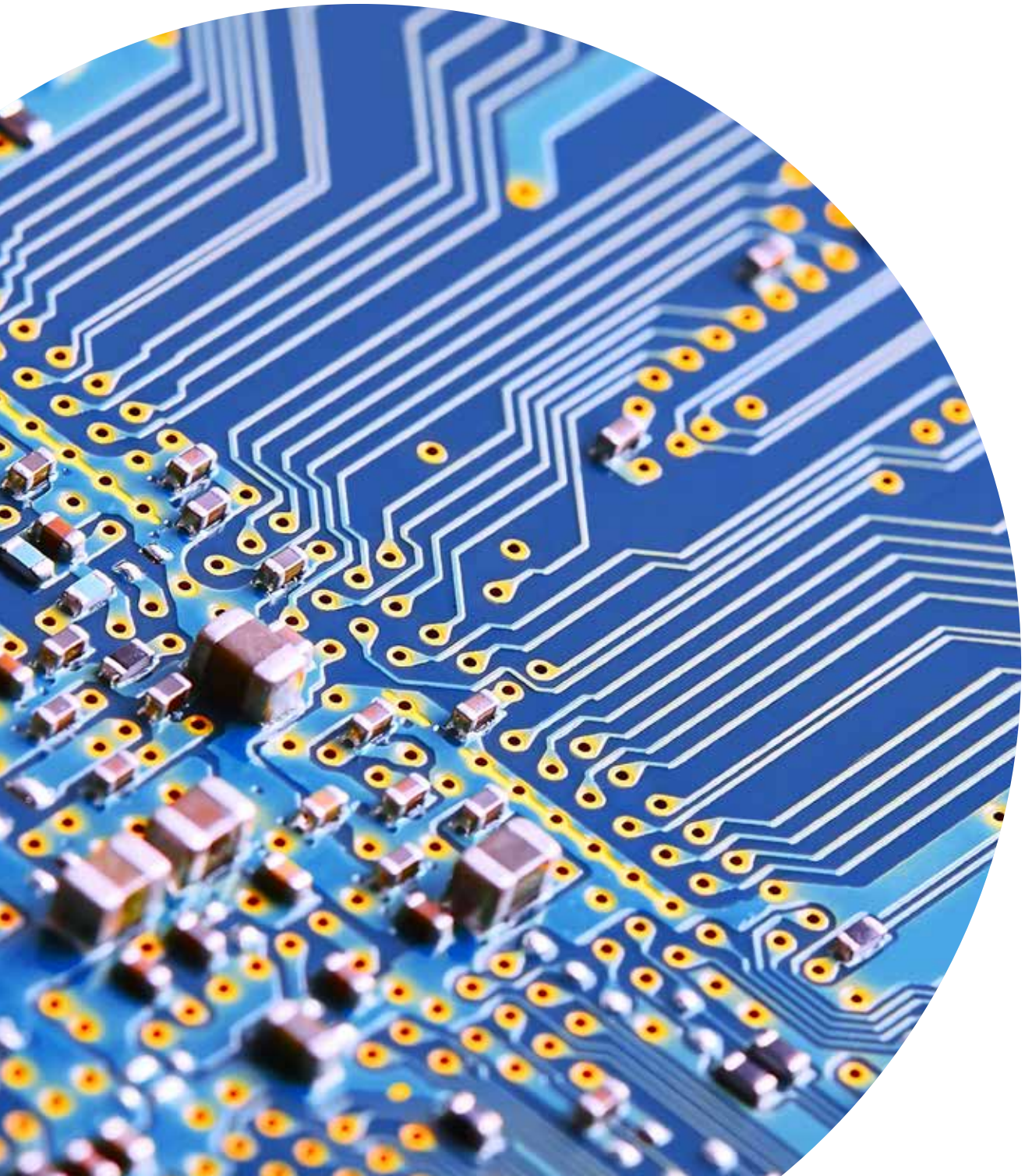
Via dit platform wil het CCB concrete resultaten behalen. Ten eerste wenst het CCB een duidelijk Belgisch Cyber Security beleid uit te tekenen. Dit houdt concrete en geteste procedures voor het behandelen van ernstige cyber security incidenten in, alsook inzicht krijgen in de actuele situatie van cyber security capaciteiten en verantwoordelijkheden in België, voorstellen lanceren tot de gewenste situatie van Cyber Security capaciteiten en verantwoordelijkheden en een actieplan opstellen om van de actuele tot de gewenste situatie te komen.

Ten tweede staat Cyber security situational awareness op de agenda. Hiervoor werd het onderplatform Cyber Intelligence opgericht. Piloot voor dit platform is de Algemene Dienst Inlichting en Veiligheid (ADIV)

Ten derde wil het CCB mechanismen oprichten voor het beheer van Cyber Security expertise en tenslotte ook het definiëren van efficiënte Cyber Security communicatieplatformen naar burgers, bedrijven en vitale sectoren.

Het Centrum voor Cybersecurity België zal een eindrapport opstellen van de bereikte resultaten en de evolutie van het beleid aansturen. Om de procedures en de capaciteiten voor het behandelen van ernstige Cyber Security incidenten permanent te kunnen evalueren zal België deelnemen aan nationale en internationale Cyber Security oefeningen.

Sinds de oprichting van het CCB is dit platform zeven keer samengekomen.



04

NATIONAAL CYBERNOODPLAN

04

ENKELE PROJECTEN WORDEN OPGESTART IN DE START-UP FASE MAAR ZULLEN PAS IN DE BUILD-UP FASE (MAART 2016-MAART 2019) IN WERKING TREDEN.

In december 2015 startte het CCB de uitwerking van een nationaal cybernoodplan. Het is cruciaal dat bij grote cyber incidenten en crisissen de verschillende Belgische diensten actief in het cyberdomein efficiënt samenwerken om de situatie zo snel mogelijk onder controle te krijgen.

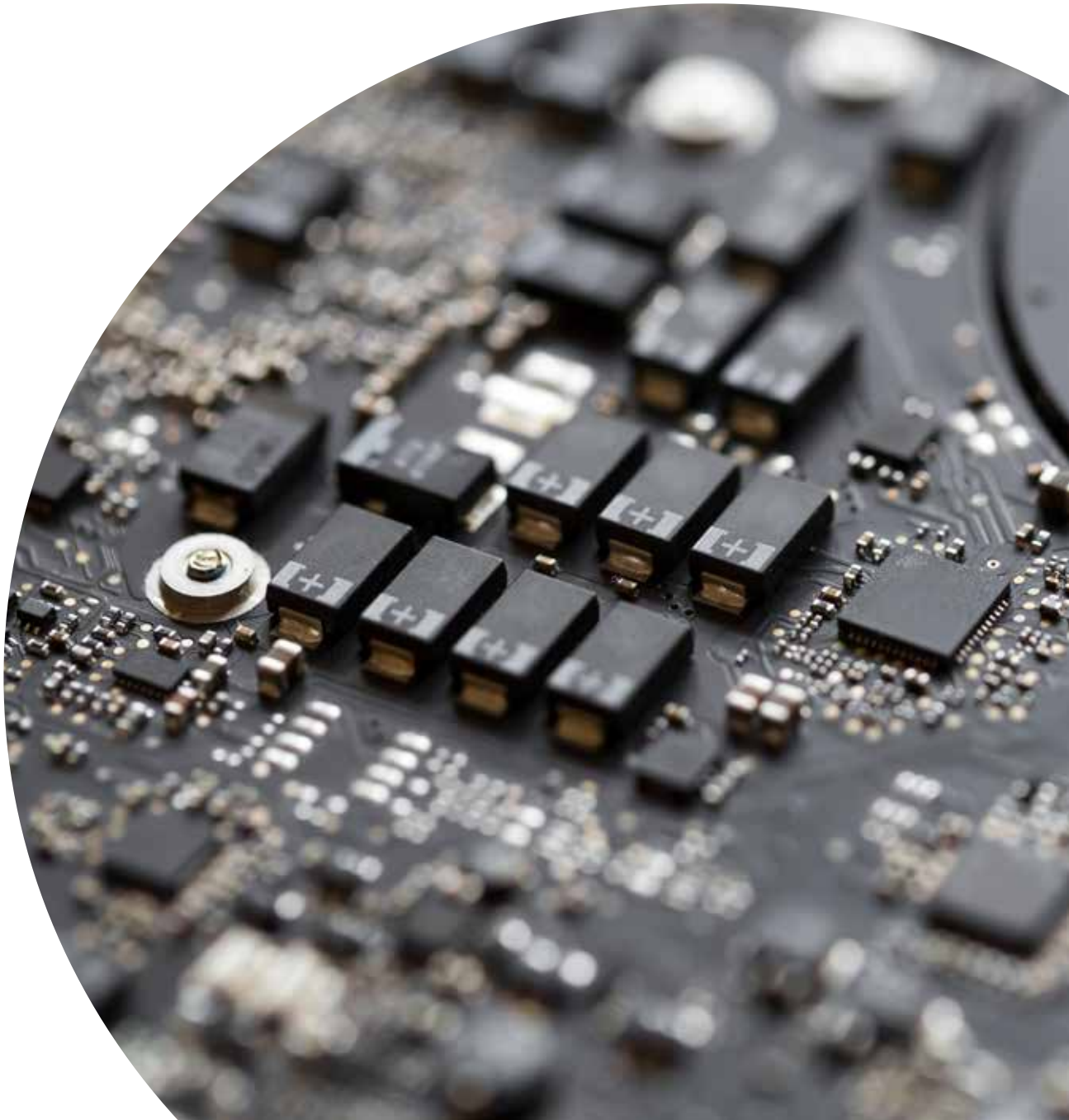
Het Belgisch nationaal cybernoodplan heeft als voornaamste doelstelling het organiseren van een antwoordstructuur op de cyber security crisissen en incidenten die een coördinatie en/of beheer op nationaal niveau vereisen. Het plan maakt een opschaling naar gelang de impact van de cybergebeurtenis. Het identificeert Nationale Cyber Security Crisissen en een Nationale Cyber Security Incidenten. Een basisescalatie wordt uitgewerkt zodat de verschillende diensten actief in het cyberdomein onderlinge acties bij het behandelen van nationale cyberincidenten op elkaar afstemmen. Er wordt veel belang gehecht aan het snel en correct doorgeven van informatie tussen de diensten onderling.

Het plan intendeert een leidraad te zijn voor de te volgen procedures en de te nemen beschermingsmaatregelen bij nationale cyber security crisissen en incidenten, wanneer daartoe de noodzaak zich voordoet. Het beschrijft de opdrachten die de verschillende organismen en diensten, ieder binnen hun wettelijke en reglementaire bevoegdheid, in voorkomend geval, dienen uit te voeren binnen het algemeen proces voor het behandelen van cyber security incidenten en crisissen.

Dit plan gaat op in een groter geheel. Elke betrokken dienst kan dit document gebruiken als basis voor de operationele aspecten van het crisis- en incidentbeheer binnen de bevoegdheden van de desbetreffende dienst.

Voor de uitwerking van dit cybernoodplan doet het CCB dankbaar beroep op de expertise en kennis van het Nationaal Crisiscentrum. De verschillende diensten die actief zijn in het cyberdomein zitten mee rond de tafel om alle actuele capaciteiten voor het behandelen van dergelijke incidenten juist weer te geven.

Tegen juni 2016 tracht het CCB een eerste versie van dit plan klaar te hebben. Oefeningen zullen worden georganiseerd om deze eerste versie te testen en het plan waar nodig bij te sturen.




CODI
CLICK
CLICK HERE FOR MORE INFOR

05

BOTNET ERADICATION SYSTEM

05

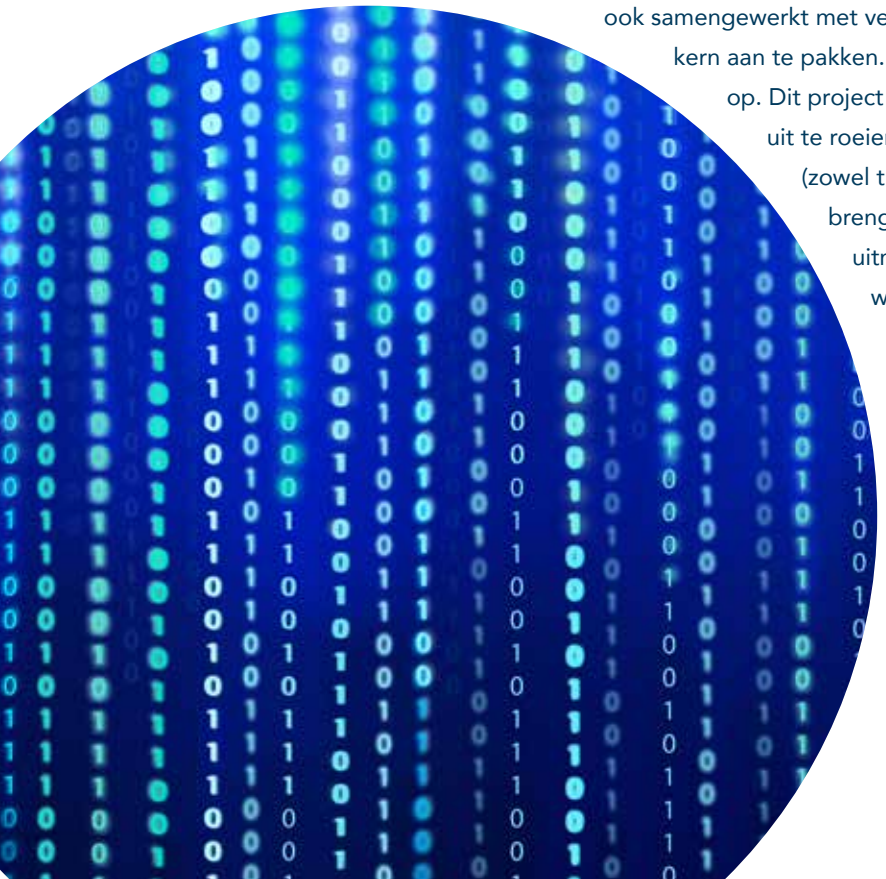
IN NOVEMBER 2015 KREEG HET CENTRUM VOOR CYBERSECURITY BELGIË HAAR VUURDOOP. OP YOUTUBE WERDEN DREIGINGEN GEUIT DIE OPRIEPEN BELGISCHE OVERHEIDSWEBSITES PLAT TE LEGGEN DOOR ZOGENAAMDE DDOS-AANVALLEN. MET EEN DDOS-AANVAL OF EEN DISTRIBUTED DENIAL-OF-SERVICE-AANVAL WORDT GEPROBEERD EEN WEBSERVER ONDERUIT TE HALEN DOOR HEM TE OVERLADEN MET EEN ZEER GROOT AANTAL PAGINAVERZOEKEN. DE SERVER KAN DEZE GROTE VRAAG NIET VERWERKEN WAARDOOR DE WEBSITE VOOR EEN TIJD NIET MEER BESCHIKBAAR ZAL ZIJN TOTDAT DE AANVAL STOPT OF DE AANVAL WORDT TEGENGEHOUDEN.

Het CCB nam de dreigingen ernstig en stuurde een waarschuwing uit naar de betrokken diensten. Op vraag van het CCB publiceerde het CERT.be naar aanleiding van de dreiging in november 2015 een whitepaper met proactieve en reactieve maatregelen tegen DDoS aanvallen. Deze whitepaper helpt wie dit wenst maatregelen te nemen tegen dit type aanval.

Het Centrum voor Cybersecurity België wil echter verder gaan dan het beschermen van overheidswebsites tegen DDOS aanvallen. De mogelijkheid om deze uit te voeren moet worden beperkt.

DDOS aanvallen worden uitgevoerd met behulp van botnets. Dit zijn uitgebreide netwerken van geïnfecteerde computers die door de aanvaller worden aangestuurd tijdens de aanval. Botnets moeten worden gedetecteerd en geïnfecteerde computers moeten worden gezuiverd.

Het CCB startte met een project Botnet Eradication System om deze botnets in België te verwijderen. Dit is een gedeelde verantwoordelijkheid en er wordt hiervoor dan ook samengewerkt met verschillende partners om het probleem bij de kern aan te pakken. Het CCB richtte een werkgroep rond het thema op. Dit project zal een belangrijke schakel zijn om botnets uit te roeien. Het doel is om geïnfecteerde gebruikers (zowel thuisgebruikers als bedrijven) op de hoogte te brengen van het feit dat zij geïnfecteerd zijn en deel uitmaken van een botnet. Naast deze informatie worden de gebruikers ook op de hoogte gebracht over mogelijke manieren om hun systeem te ‘ontsmetten’. Er wordt nauw samengewerkt met de privacycommissie om de gebruikers van geïnfecteerde computers correct op de hoogte te stellen.



Dit project werd in maart 2016 gestart.

06

DE NIS RICHTLIJN

06

ONTWERP VAN EUROPESE RICHTLIJN HOUDENDE MAATREGELEN OM EEN HOOG GEMEENSCHAPPELIJK NIVEAU VAN NETWERK- EN INFORMATIEVEILIGHEID TE WAARBORGEN (NIS)

Eind 2015 werd een ontwerp van richtlijn houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatieveiligheid te waarborgen ("Network and Information systems Security" – afgekort NIS) afgewerkt binnen de Europese instellingen.

De doelstelling van de richtlijn is om een hoog gemeenschappelijk niveau te waarborgen voor de beveiliging van de netwerken en informatiesystemen binnen de Europese Unie teneinde de werking van de interne markt te verbeteren.

De voorziene maatregelen beogen de doeltreffendheid van de digitale informatiesystemen te verbeteren, de cybercriminaliteit te bestrijden en het internationaal beleid inzake cybersecurity en de cyberdefensie van de EU te versterken.

De voorgestelde richtlijn inzake beveiliging van de netwerken en informatiesystemen is een belangrijk onderdeel van de uitvoering van de Europese cyberstrategie (goedgekeurd op 07/02/2013) en verplicht alle lidstaten, exploitanten van kritieke diensten (actoren in de domeinen van energie, transport, banken, gezondheidszorg en drinkbaar water) en de leveranciers van digitale diensten (online markt, online zoekmachines, clouddiensten) om in de volledige EU te zorgen voor een veilige en betrouwbare digitale omgeving.

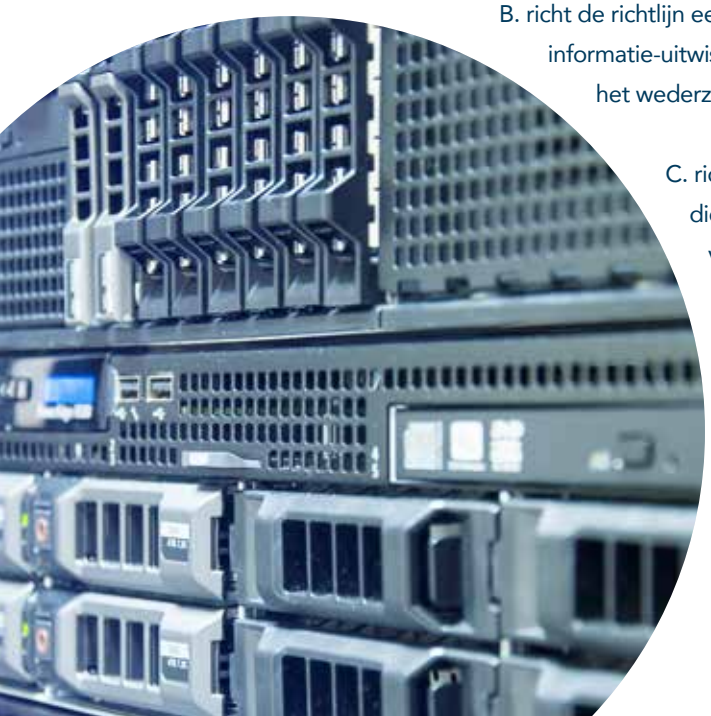
Daartoe:

A. legt de richtlijn verplichtingen vast voor alle lidstaten wat betreft de goedkeuring van een nationale strategie inzake beveiliging van de netwerk- en informatiesystemen;

B. richt de richtlijn een samenwerkingsgroep op om de strategische samenwerking en de informatie-uitwisseling tussen de lidstaten te bevorderen en te vereenvoudigen en het wederzijdse vertrouwen te versterken;

C. richt de richtlijn een netwerk op van responsteams voor incidenten die de digitale veiligheid schaden (CSIRT) om bij te dragen aan de versterking van het vertrouwen tussen de lidstaten en om een snelle en effectieve samenwerking te bevorderen op operationeel niveau;

D. stelt de richtlijn vereisten op inzake veiligheid en kennisgeving voor de exploitanten van kritieke diensten en voor de leveranciers van digitale diensten;



E. legt de richtlijn verplichtingen vast voor de lidstaten voor de aanduiding van bevoegde nationale autoriteiten, unieke loketten en CSIRT belast met taken met betrekking tot de beveiliging van de netwerk- en informatiesystemen.

De cybersecuritystrategie en de bijbehorende richtlijn zijn belangrijke bouwstenen voor een veilige digitale omgeving in Europa. Cybersecurity vereist niet alleen samenwerking tussen verschillende actoren van de publieke en de privésector en binnen de lidstaten. We moeten ook meer aandacht schenken aan wat er gebeurt aan de andere kant van onze grenzen om er oplossingen te zoeken en ICT-verstoringen en cyberaanvallen te voorkomen.

Het CCB heeft het uitwerkingsproces van dit ontwerp van richtlijn aandachtig opgevolgd en zal, zodra deze richtlijn is goedgekeurd, instaan voor de coördinatie van het opstellen van de ontwerpwetteksten die noodzakelijk zijn voor de omzetting ervan in Belgisch recht.

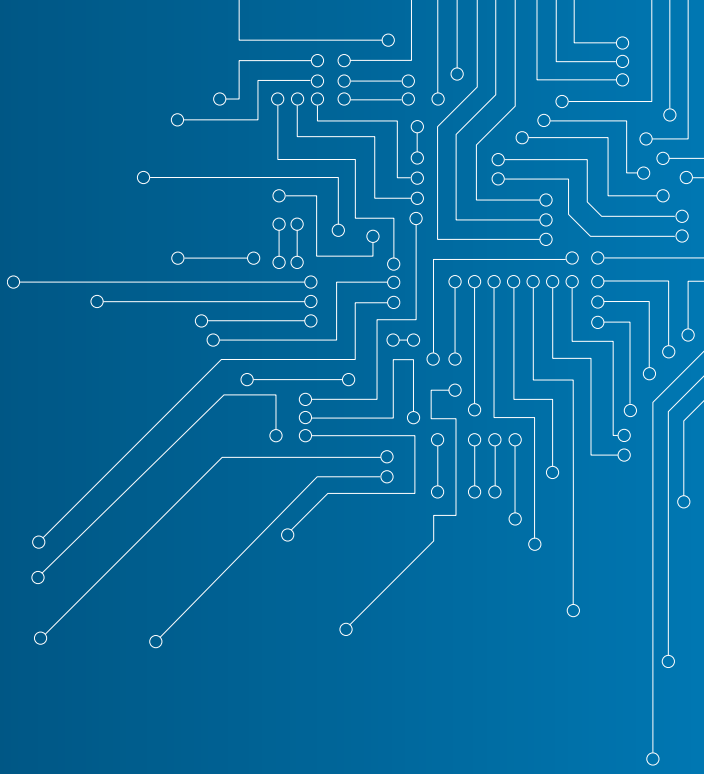
07

EARLY WARNING SYSTEM

OM DE VITALE SECTOREN IN BELGIË OP EEN SNELLE EN GESTANDAARDISEERDE MANIER TE WAARSCHUWEN OVER NIEUWE CYBERDREIGINGEN EN -AANVALLEN, RICHT HET CCB EEN EARLY WARNING SYSTEEM OP.

Via een gedeeld platform zullen Vitale Sectoren toegang krijgen tot gefilterde waarschuwingen voor intrusies en andere cyberdreigingen. Zo kunnen zij snel informatie krijgen van een betrouwbare bron en zo zeer snel actie ondernemen.
Er wordt verwacht dat dit najaar nog het Early Warning Systeem in werking zal treden.

CENTRE FOR
CYBER SECURITY
BELGIUM



CENTRE FOR
CYBER SECURITY BELGIUM
Wetstraat, 16 - 1000 Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

CHANCELLERY OF
THE PRIME MINISTER

.be