**Persbericht 19 februari 2018**

“Het Centrum voor Cybersecurity België bouwt verder aan een cyberveilig België”

**2.5 jaar CCB - een overzicht**

In juli 2015 werd het Centrum voor Cybersecurity België opgericht. Het centrum is nog in volle opbouwfase maar kan vandaag al heel wat realisaties en nieuwe plannen voorleggen. De aanwerving van het nodige personeel om de doelstellingen te realiseren was dan ook een belangrijk project.

Het CCB telt momenteel **10 medewerkers**: een directeur en adjunct-directrice, 4 project managers, een juridisch adviseur, een communicatieverantwoordelijke en twee office managers.

In januari 2017 werd het nationale Computer Emergency Response Team (CERT) onder het bestuur van het CCB geplaatst.

Om de opdrachten van CERT.be goed te kunnen uitoefenen heeft het CCB in 2017 heel wat medewerkers aangetrokken. Eind 2017 telde CERT.be een 20-tal personeelsleden waaronder een directeur, een program manager, een technology advisor, een communicatieverantwoordelijke, cyberanalisten en – experten, en een office manager.

De laatste aanwervingen worden momenteel gefinaliseerd, CERT.be zal dan 24 medewerkers tellen.

Bovendien heeft de regering besloten om CERT.be verder uit te breiden tot **36 experts in 2019**.

In de 2de helft van 2018 zal CERT.be 24 uur per dag beschikbaar zijn voor bedrijven en vitale sectoren, dit om aan een bestaande behoefte te beantwoorden en om vragen tijdig te verwerken.

Twee en een half jaar CCB zijn niet onopgemerkt voorbij gegaan en de inspanningen worden nog versterkt.

**CIJFERS IN DE KIJKER:**

* Uitbreiding CCB en CERT.be naar in totaal **34 medewerkers**
* In 2017 organiseerde het CCB **36** cyberveiligheidsopleidingen binnen de overheid: **437** ambtenaren namen deel.
* De campagne tegen phishing is opgepikt door ongeveer **2 miljoen** internetgebruikers
* **150.000 berichten** verstuurd naar verdacht@safeonweb.be
	+ **9%** van de internetgebruikers verloor al eens geld door internetfraude
	+ **65%** van de internetgebruikers zegt het afgelopen jaar een verdacht bericht ontvangen te hebben met de vraag om op een link te klikken of een bijlage te openen
* Nieuwe online referentiegids rond cyberveiligheid met zowel basisvoorzieningen als meer geavanceerde acties, gebundeld in **4 categorieën** en meer dan **150 maatregelen**

	+ In 2016 werd **twee derde** van de Belgische bedrijven slachtoffer van cybercriminaliteit.
	+ Voor de meeste bedrijven bleef de schade beperkt tot een verstoring van de dagelijkse werking maar voor 9% van de door cyberafpersing en –chantage getroffen bedrijven liep de schade op tot meer dan 10.000 euro. (bcc-project.be, 29/6/2017)

Cyberveiligheidsopleidingen binnen de overheid

In 2017 voorzag het Centrum voor Cybersecurity België 36 verschillende opleidingen in cyberveiligheid, voorzien voor 437 ambtenaren.

Deelnemers die een opleiding volgden kwamen uit volgende overheidsorganisaties:

|  |
| --- |
| * FOD Kanselarij
 |
| * FOD Werkgelegenheid
 |
| * FOD Justitie
 |
| * FOD Economie
 |
| * FOD Binnenlandse Zaken
 |
| * FOD Mobiliteit
 |
| * FOD Beleid en Ondersteuning
 |
| * FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu
 |
| * FOD Sociale zekerheid
 |
| * FOD Financien
 |
| * FOD Buitenlandse Zaken
 |
| * POD Wetenschapsbeleid
 |
| * POD Maatschappelijke Integratie, Armoedebestrijding, Sociale Economie en Grootstedenbeleid
 |
| * Defensie
 |
| * Federale Politie
 |

Daarnaast kregen de cybercrime magistraten van het Federaal Parket de mogelijkheid een intensieve Cybersecurity Essentials bootcamp te volgen.

Campagne Safeonweb 2017 ging met succes de strijd aan tegen phishing

Op 2 oktober 2017 lanceerden het Centrum voor Cybersecurity België en de Cyber Security Coalition een sensibiliseringscampagne rond cyberveiligheid in het kader van de European Cyber Security Month.

“Met deze campagne wilden we alle internetgebruikers wapenen tegen phishing. We wilden bereiken dat de internetgebruiker weet dat niet elk bericht dat hij of zij per e-mail of via social media krijgt, ook echt is”, stelt Miguel De Bruycker, directeur CCB. “Er circuleren veel valse berichten en we wilden dat mensen deze herkennen, er zeker niet op reageren, bijlages openen of op links klikken. Maar we verwachtten nog meer. We vroegen iedereen om verdachte berichten door te sturen naar verdacht@safeonweb.be en ze vervolgens te wissen.“

Zowel het bereik als de resultaten van de campagne zijn positief

Met de advertenties op Facebook en Instagram alleen al bereikten we tijdens de campagnemaand 1.000.000 mensen van alle leeftijden en van beide landstalen. 830.000 mensen zagen de advertenties in de bioscoop en meer dan 1 miljoen in de krant. Kijkers van onder meer één, Canvas en RTL zagen in prime time de tv-spotjes. 20% van de respondenten van onze meting zegt spontaan de campagne opgemerkt te hebben. Daaruit kunnen we afleiden dat ze opgepikt is door ongeveer 2 miljoen internet-gebruikers. Meer dan 130.000 mensen bezochten de website [www.safeonweb.be](http://www.safeonweb.be) en 4000 daarvan deden de grote phishingquiz.

Stuur verdachte berichten naar verdacht@safeonweb.be

Maar we wilden meer bereiken met deze campagne. Daarom vroegen we de internetgebruiker om ons verdachte berichten te bezorgen. De links en bijlages van deze berichten worden automatisch gescand met geavanceerde anti-virustechnologie. De oproep werd massaal opgevolgd en tot op vandaag krijgen we nog steeds een 600-tal berichten per dag doorgestuurd. In totaal kregen we ongeveer 150.000 e-mails te verwerken. Op die manier blokkeren we dagelijks 3 à 4 nieuwe phishingwebsites.

**NIEUWE REALISATIE IN DE KIJKER:**

# Geef cybercriminelen geen kans in 2018

## Om bedrijven en organisaties beter te wapenen tegen cyberaanvallen publiceren wij een online referentiegids.

Criminelen die uit zijn op financieel voordeel of die schade willen berokkenen aan bedrijven slaan steeds vaker online hun slag. Bedrijven van hun kant zijn in toenemende mate afhankelijk van ICT en online verkoop, waardoor ze kwetsbaar zijn voor cybercriminaliteit. In 2016 werd twee derde van de Belgische bedrijven slachtoffer van cybercriminaliteit. Voor de meeste bedrijven bleef de schade beperkt tot een verstoring van de dagelijkse werking maar voor 9% van de door cyberafpersing en –chantage getroffen bedrijven liep de schade op tot meer dan 10.000 euro. (bcc-project.be, 29/6/2017)

## Goed voornemen 2018: maak een cybersecurityplan

Voor sommige bedrijven en organisaties lijkt de stap naar een uitgewerkt cyberveiligheidsbeleid onoverkomelijk.

“Ze hebben onvoldoende inzicht in de gevaren, geen expertise in de materie, ze denken dat het hen niet zal overkomen of ze gaan ervan uit dat de investering niet zal lonen. Toch raden wij elke organisatie aan om bij wijze van goed voornemen voor 2018 een **cybersecurityplan** uit te werken”, aldus Miguel De Bruycker, directeur Centrum voor Cybersecurity België.

Deze referentiegids zal hen helpen om van start te gaan. De gids werd opgesteld door het Centrum voor Cybersecurity België, in samenwerking met de FOD Economie en de Cyber Security Coalition Belgium en staat ter beschikking op de website van het CCB. www.ccb.belgium.be



# CONTACT – Niet voor publicatie

## Over het Centrum voor Cybersecurity België:

Het Centrum voor Cybersecurity België (CCB) is het nationale centrum voor cyberveiligheid in België. Het CCB stelt tot doel het superviseren, het coördineren en het waken over de toepassing van de Belgische strategie betreffende cyberveiligheid. Door het optimaliseren van de informatie-uitwisseling zullen de bevolking, de bedrijven de overheid en de vitale sectoren zich gepast kunnen beschermen.

[www.ccb.belgium.be](http://www.ccb.belgium.be)

**Perscontact Centrum voor Cybersecurity België**

|  |  |
| --- | --- |
| Andries Bomans T: +32 471 66 00 06Andries.bomans@ccb.belgium.be  |  |