

# Persbericht

## Sensibiliseringscampagne cybsersecurity

Brussel, 1/10/2018

### Oktober: maand van de cybersecurity

In het kader van de **European Cyber Security Month** lanceren wij (het Centrum voor Cybersecurity België en de Cyber Security Coalition) voor de 4<sup>de</sup> keer een **sensibiliseringscampagne** rond **cyberveiligheid**. Deze keer willen we de internetgebruiker aansporen om regelmatig **back-ups te maken en updates uit te voeren**.

Tijdens de campagnemaand oktober willen we de aandacht vestigen op het thema via radiospotjes en filmpjes op social media. Op de campagnewebsite bij <https://campagne.safeonweb.be/nl> bieden we niet alleen informatie maar ook een digitale gezondheidsindex aan. We gaan met onze boodschap ook letterlijk naar de burger toe: we houden op 9 oktober een actie in 5 grote treinstations en we gaan 10 dagen op tour met de federal truck.

**Evy Gruyaert** en **Julie Taton** zijn de digitale gezondheidscoaches bij deze campagne.

*Met de federal truck gaan wij naar de bevolking toe. Op 10 verschillende plaatsen in Brussel, Vlaanderen en Wallonië houden we halt en nodigen we iedereen uit om meer te weten te komen over updates en back-ups, aldus Phédra Clouner, vicedirecteur CCB.*

### Waarom zijn back-ups en updates zo belangrijk?

Op 12 mei 2017 werd de wereld opgeschrikt door de uitbraak van de ransomware WannaCry. De snelheid waarmee het gijzelvirus systemen wereldwijd infecteerde, was ongezien. In 150 landen werden meer dan 300.000 toestellen geïnfecteerd. Het virus kon zo snel en hard toeslaan door gebruik te maken van een gekende kwetsbaarheid in IT-systemen.

*Miguel De Bruycker, directeur CCB: Een gekende kwetsbaarheid in een IT-systeem kan je eenvoudig verhelpen door software-updates uit te voeren. De impact van aanvallen zoals ransomware kan worden beperkt als organisaties en burgers snel hun systemen updaten. Op safeonweb.be bieden wij tips en tools aan die je helpen om al je systemen steeds up to date te houden.*

Ransomware is een gijzelvirus dat je toestel en bestanden gijzelt en losgeld vraagt. Slachtoffers van Wannacry werden verplicht te betalen om hun gegevens terug te krijgen.

Organisaties en personen die een **back-up** hadden van hun gegijzelde gegevens konden zonder het betalen van losgeld de schade aanzienlijk beperken.

Jan De Blauwe, voorzitter Cyber Security Coalition:

*Het maken van een back-up van de belangrijkste data kan professionele schade in geval van verlies of incident aanzienlijk verminderen.*

*Elke organisatie zou daarom een goede back-up of Disaster Recovery oplossing moeten voorzien om business continuïteit te kunnen waarborgen.*

Ook de gewone internetgebruiker heeft veel te verliezen.

*Anthony (54) verloor tien jaar werk: Op 18 juni tijdens de wedstrijd Panama-België heb ik mijn laptop verloren. Op een onbewaakt moment heeft een onbekende mijn schoudertas meegenomen, met mijn laptop en een externe harde schijf waarop al mijn projecten staan. Die harde schijf bevat tien jaar werk en persoonlijke bestanden. Het lijkt alsof ik een man zonder verleden ben geworden.*

## Nood aan een digitale gezondheidsboost?

Uit onze cijfers (sept 2018, n=400) blijkt dat:

- 22% van de respondenten nooit een back-up maakt
- Wie wel eens een back-up maakt doet dat onregelmatig (29%)
- 14% maakt een back-up op het toestel zelf, wat weinig zinvol is.
- ¼ van de respondenten voert nooit (5%) of zelden (19%) updates uit.

Hoog tijd voor wat digitaal gezondheidsadvies! Want de risico's beperken is eigenlijk heel eenvoudig. En toch doen we het niet altijd. Opmerkelijk, want we zijn toch ook begaan met onze fysieke gezondheid, niet? Voldoende beweging, gezonde voeding: je kent het wel. Maar werken we ook aan onze digitale gezondheid?

Uit onderzoek blijkt alvast dat het niet zo goed gesteld is met de digitale gezondheid van de Belgen. Meer zelfs: buurlanden als Frankrijk, Duitsland en Nederland doen het beter dan wij.

Laten we dat zomaar gebeuren? <https://youtu.be/BxxgZrlvwnl>

*Wat ons betreft alleszins niet.* CCB lanceert daarom de digitale gezondheid index. Vanaf nu kan je met een eenvoudige test uitzoeken hoe het met zijn digitale gezondheid staat. Heb je nog werkpuntjes, dan ontvang je tips op maat om je digitale gezondheid te boosten. Samen maken we van België het digitaal gezondste land! <https://campagne.safeonweb.be/nl>

---

## Achtergrond

### 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. Meer info op [www.ccb.belgium.be](http://www.ccb.belgium.be)

### Perscontact Centrum voor Cybersecurity België

Andries Bomans  
T: +32 471 66 00 06  
[Andries.bomans@ccb.belgium.be](mailto:Andries.bomans@ccb.belgium.be)

Katrien Eggers  
T: +32 485 76 53 36  
[Katrien.eggens@cert.be](mailto:Katrien.eggens@cert.be)

### Over de Cyber Security Coalition:

De *Cyber Security Coalition* heeft als missie de Belgische cyberveiligheid weerbaarder te maken door een sterk ecosysteem voor cyberbeveiliging op nationaal niveau uit te bouwen. Dit is mogelijk door de vaardigheden en expertise van de academische wereld, bedrijven en de overheid samen te brengen in een op vertrouwen gebaseerd platform dat zich focust op het bevorderen van informatie-uitwisseling, operationele samenwerking, het formuleren van aanbevelingen voor efficiëntere beleidslijnen en richtlijnen, en tenslotte het uitvoeren van gezamenlijke bewustmakingscampagnes voor burgers en organisaties.

Perscontact Cyber Security Coalition  
Sofie De Moerlose  
T: 0478 78 96 07  
[info@cybersecuritycoalition.be](mailto:info@cybersecuritycoalition.be)