

02 okt 2026 -11:25

## Geen toegang voor cybercriminelen: CCB lanceert Gesloten Bedrijvendag

Op 5 oktober, de dag na 'Open Bedrijvendag', roept het Centrum voor Cybersecurity België op om de deuren van organisaties en bedrijven weer te sluiten. Niet voor het grote publiek, wel voor cybercriminelen. Met Gesloten Bedrijvendag krijgt online veiligheid voor bedrijven extra aandacht. En dat is nodig. ⇒ (ONDER EMBARGO tot maandag 5 oktober 7:00)

Artificiële Intelligentie (AI) maakt cyberaanvallen mogelijk die voorheen ondenkbaar waren. AI-modellen sporen kwetsbaarheden op aan een razend tempo en proberen op die manier toegang te krijgen tot systemen van bedrijven.



Miguel De Bruycker  
Directeur-Generaal Centrum voor Cybersecurity België



Vandaar de oproep naar bedrijven om met de hulp van Safeonweb at Work 24/7 de deuren gesloten te houden. Niet voor het grote publiek, wel voor cybercriminelen.

Allemaal goed en wel, maar hoe begin je daar als bedrijf dan aan?

Via Safeonweb at Work kunnen bedrijven en organisaties, groot en klein, richtlijnen vinden om zowel de eerste stappen te nemen naar een veiligere IT-infrastructuur als ook gevorderde beveiliging op poten te zetten. In enkele stappen, zijn de online poorten van je organisatie morgen al gesloten voor cybercriminelen.

### Stap 1: Stel de basisbeveiliging vandaag nog op orde

De beste bescherming blijft een sterke basisbeveiliging.

Alles start met een goede basisbeveiliging voor iedereen.

- Wie niet weet waar te beginnen, duikt nu in de online diagnosetool. In enkele kliks, weet je waar beginnen: <https://atwork.safeonweb.be/nl/online-diagnose>
- Het echte werk begint als je het gratisCyfun Framework als leidraad gebruikt om de basis op orde te krijgen: <https://cyfun.eu>

## Stap 2: Blijf altijd op de hoogte

Registreer je organisatie vandaag en krijg gratis in real time waarschuwingen voor potentiële bedreigingen en kwetsbaarheden in je netwerk. Detecteer, beoordeel en beperk kwetsbaarheden op je domein. <https://atwork.safeonweb.be/nl/register-my-organisation>

## Stap 3: Investeer

Leer financiële ondersteuningsmogelijkheden kennen:

<https://atwork.safeonweb.be/nl/tools-resources/ondersteunende-maatregelen>

|| Je bedrijf 24/7 gesloten houden voor cybercriminelen is geen sinecure. Het vraagt naast inzet en prioriteiten stellen ook een belangrijke investering. We moeten daar niet flauw over doen. Het goede nieuws is dat er tal van mogelijkheden zijn om financiële ondersteuning te vragen, ook op jouw maat. We zetten je graag op weg. ||



Ellen Stassart  
Head of the National Cybersecurity Coordination Centre Belgium (NCC-BE)

## Enkele cijfers:

In 2026 kreeg het CCB al 588 meldingen (1/1 - 28/9) tegenover 635 in 2025 (hele jaar)

## Waaronder:

|                           |     |
|---------------------------|-----|
| Inbreuk op een account    | 156 |
| Inbreuk op het IT-systeem | 97  |

|            |    |
|------------|----|
| Ransomware | 80 |
| Datalek    | 47 |
| CEO-fraude | 21 |

## Wat is het Centrum voor Cybersecurity België?

Het Centrum voor Cybersecurity België is de nationale autoriteit voor cyberveiligheid in België. Het superviseert, coördineert en waakt over de toepassing van de Belgische cyberveiligheidsstrategie. Door optimale informatie-uitwisseling kunnen bedrijven, de overheid, aanbieders van essentiële diensten en de bevolking zich gepast beschermen.

Persmoment: enkel op afspraak!

Bedrijven openden hun deuren afgelopen zondag, maar vandaag roepen we op tot een gesloten bedrijven dag. Wil je weten waarom? Interview met Miguel De Bruycker, directeur-generaal van het CCB mogelijk op afspraak.

Centrum voor Cyber Security België  
Wetstraat 18  
1000 Brussel  
België  
<http://www.ccb.belgium.be>

Katrien Eggers  
Woordvoerder(NL/FR/E)  
+32 485 76 53 36  
[katrien.eggerts@ccb.belgium.be](mailto:katrien.eggerts@ccb.belgium.be)

Michele Rignanese  
Woordvoerder(NL/FR/E)  
+32 (0)477 38 87 50  
[michele.rignanese@ccb.belgium.be](mailto:michele.rignanese@ccb.belgium.be)