

17 März 2025 -06:02

## Größte Operation zur Cybersicherheit in Belgien: 2410 Organisationen aus kritischen Sektoren ergreifen Maßnahmen

Seit der Einführung der NIS2-Gesetzgebung im Oktober letzten Jahres haben sich 2410 Organisationen aus kritischen Sektoren beim Zentrum für Cybersicherheit Belgien (CCB) registriert. Derzeit läuft die bisher größte Cybersicherheitsoperation des Landes. In diesem Zeitraum sind die Meldungen über Cyber-Vorfälle um 80% gestiegen.

Die Cyberkriminalität wird in den kommenden Jahren explodieren. Die neue europäische Richtlinie zur Netz- und Informationssicherheit (NIS2) zielt darauf ab, die Cybersicherheit und die Widerstandsfähigkeit von wesentlichen und wichtigen Diensten in genau definierten Sektoren in der EU zu verbessern.

Belgien war der erste europäische Mitgliedsstaat, der die neue NIS2-Richtlinie vollständig umgesetzt hat. Belgische Organisationen, die unter die NIS2-Gesetzgebung fallen, haben bis morgen Zeit, sich auf der Website [atwork.safeonweb.be](https://atwork.safeonweb.be) verbindlich zu registrieren und ergreifen derzeit die notwendigen Sicherheitsmaßnahmen wie den Schutz vor Cyberangriffen und Datenschutzverletzungen.

### Wer hat sich heute schon registriert

Insgesamt haben sich mehr als 4500 Organisationen aus allen Sektoren registriert. Bis heute haben sich 2410 NIS2-Organisationen aus kritischen Sektoren wie Energie, Verkehr, Gesundheitswesen, digitale Infrastruktur, Regierung, Fertigung usw. registriert.

Eine Schätzung auf der Grundlage von Zahlen des FÖD Wirtschaft bringt uns zu einer Gesamtzahl von etwa 2.500 Organisationen, die in den Anwendungsbereich der NIS2 fallen. Wir können also sagen, dass die große Mehrheit sich rechtzeitig angemeldet hat.

"Wir gehen davon aus, dass die Zahl der Registrierungen von NIS2-Organisationen und der Meldungen von Cybervorfällen oder -bedrohungen in den kommenden Monaten weiter steigen und sich später stabilisieren wird. Die betroffenen Organisationen in unserem Land arbeiten hart daran, ihre Cybersicherheit auf die nächste Stufe zu heben." sagte Miguel De Bruycker, Generaldirektor des Centre for Cybersecurity Belgium (CCB).

### Meldung von Vorfällen nimmt zu

In den letzten 18 Monaten gingen beim CCB insgesamt 556 Berichte über Cybervorfälle ein. Von August 2023 bis September 2024 erhielten wir durchschnittlich 25 Meldungen pro Monat. Seit der Einführung der NIS2-Gesetzgebung im letzten Jahr gab es 226 Vorfälle, also durchschnittlich 45 pro Monat. Das sind 80% mehr als in der Zeit davor. Die Meldung von Vorfällen hat aufgrund der Umsetzung der NIS2-Gesetzgebung zugenommen. Es gibt keine Anzeichen dafür, dass es tatsächlich mehr Cyberangriffe auf belgische Organisationen gibt.

"Wir stellen fest, dass sich die Organisationen in der Vergangenheit nicht auskannten oder es nicht für nötig hielten, Vorfälle zu melden", erklärt Miguel De Bruycker. "Es gab in der Vergangenheit eine Untererfassung. Die Zahl der signifikanten Meldungen hat nicht per se zugenommen."

Eine registrierte Organisation hat einen Wert von 2

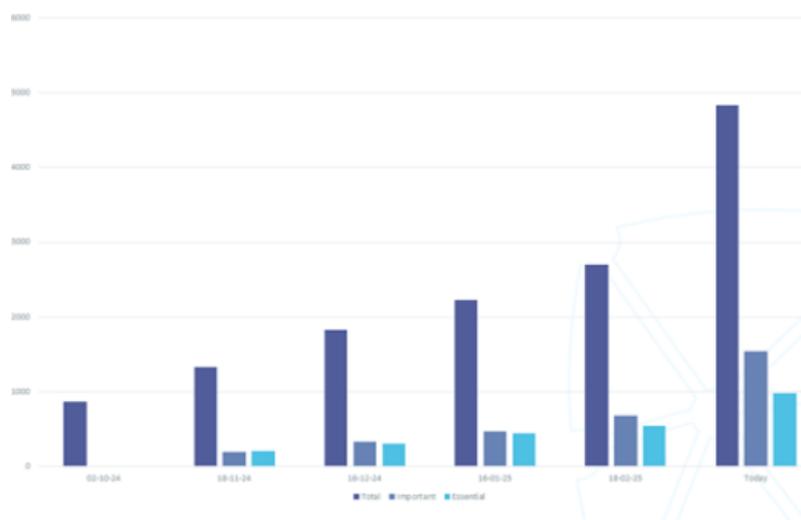
Nicht nur NIS2-Organisationen können sich registrieren. [Die Registrierung von bei Safeonweb@Work](#) bietet auch allen anderen Organisationen viele Vorteile.

"Im Februar 2025 wurden wir mit einem Cyberangriff konfrontiert, und dank unserer Registrierung konnten wir auf ein schnelles und effizientes Eingreifen der CCB zählen. Die Nützlichkeit der Registrierung hat sich seitdem bewährt. Auch die zusätzlichen Dienstleistungen sind sehr nützlich", erklärt Dirk Declerck, CEO des Hafens von Ostende.

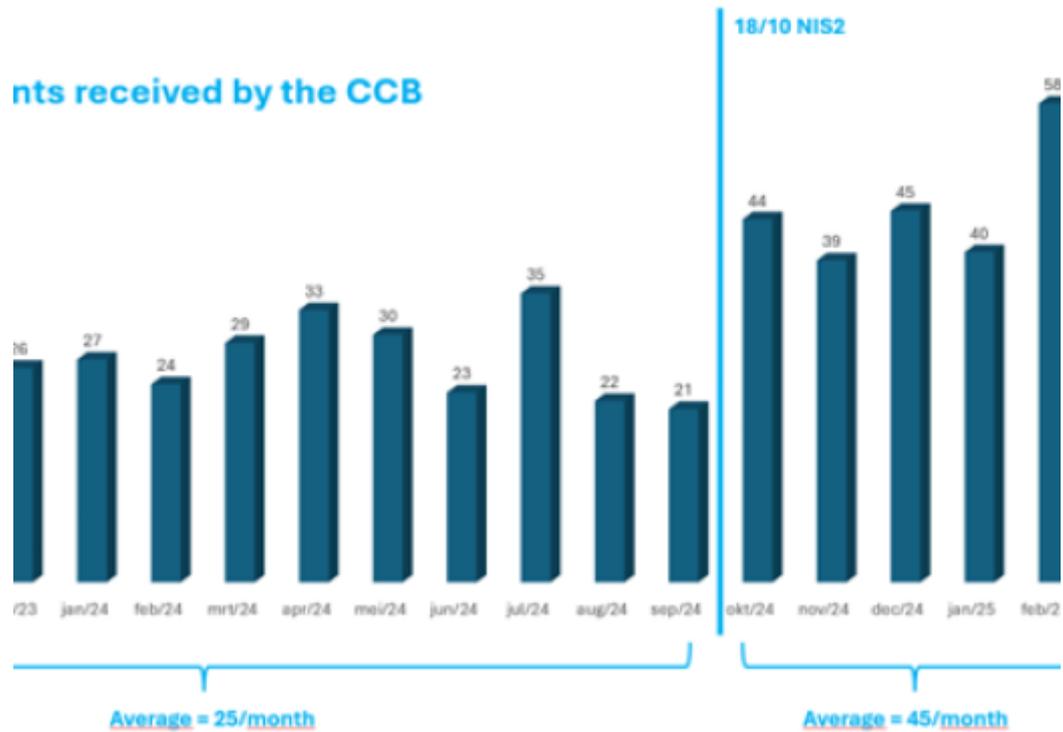
Registrierte Organisationen erhalten kostenlosen Zugang zu den folgenden Diensten:

- **Priorität:** Nach Ihrer Registrierung verfügen wir über einige grundlegende Daten. Wenn wir ein verwundbares System auf einem Domännennamen oder einer IP-Adresse entdeckt haben, die registriert ist, können wir Ihre Organisation sehr schnell alarmieren. NIS2-Organisationen haben jedoch Vorrang vor anderen Organisationen.
- **Cyber Threat Alerts:** unterstützt Unternehmen bei der Untersuchung und Eindämmung potenzieller Cyber-Bedrohungen in ihrem Netzwerk, indem sie strukturelle Benachrichtigungen über Schwachstellen und Infektionen erhalten.
- **Quick Scan Report:** Unternehmen erhalten einen Bericht, der einen Überblick über Sicherheitsschwächen und Verbesserungsmöglichkeiten bietet.
- **Selbsteinschätzung:** ein kurzer Fragebogen, um Schwachstellen zu ermitteln und gezielte Empfehlungen zu erhalten
- **Richtlinienvorlagen:** vorgefertigte Cybersicherheitsrichtlinien.

## gistration Evolution



## Registration



## Incidents

Zentrum für Cybersecurity Belgien  
Rue de la Loi 18  
1000 Brüssel  
Belgien  
<http://www.ccb.belgium.be>

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

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