18 Okt. 2024 -03:00

Belgien setzt Maßstäbe: Erster Mitgliedstaat, der die neuen europäischen Vorschriften zur Cybersicherheit (NIS2) vollständig umsetzt

Unternehmen können jetzt richtig zur Sache kommen

Belgien ist der erste europäische Mitgliedstaat, der die neuen NIS2-Vorschriften vollständig umsetzt. Diese Regeln stärken das Niveau der Cybersicherheit erheblich. Schätzungsweise mindestens 2.500 belgische Organisationen sind ab heute verpflichtet, sich auf der Website atwork.safeonweb.be zu registrieren und Sicherheitsmaßnahmen zu ergreifen. Damit haben sie den Schlüssel in der Hand, um ihre Cybersicherheit auf die nächste Stufe zu heben.

Bei Angriffen mit Ransomware und Datendiebstahl werden anfällige Organisationen täglich Opfer von Cyberkriminellen, die sichtbare Sicherheitslücken oder das Fehlen einer Zwei-Schritt-Verifizierung (2FA) ausnutzen. Die neue europäische Richtlinie für Netz- und Informationssicherheit (NIS2) soll dem einen Riegel vorschieben. Sie soll die Widerstandsfähigkeit der EU-Länder gegen Cyberbedrohungen erhöhen und wurde in Belgien in das NIS2-Gesetz umgesetzt.

Positive Auswirkungen auf die Cybersicherheit

"Derzeit sind bereits rund 200 Organisationen bei uns registriert, aber wir gehen davon aus, dass diese Zahl in den kommenden Wochen stark ansteigen wird", sagte Miguel De Bruycker, Generaldirektor des Centre for Cybersecurity Belgium (CCB), gegenüber IANS.

"Die NIS2-Gesetzgebung dehnt die bestehenden Cybersicherheitsregeln auf weitere Sektoren aus. Organisationen sollten NIS2 nicht als Belastung sehen, sondern als Chance, ihre Widerstandsfähigkeit zu stärken", sagt Valéry Vander Geeten, Leiter der Rechtsabteilung des Centre for Cybersecurity Belgium (CCB). "Die Gesetzgebung unterscheidet zwischen Schlüssel- und wesentlichen Organisationen, je nach Sektor und Größe."

Von einigen Ausnahmen abgesehen, gilt das NIS2-Gesetz für Organisationen einer bestimmten Größe, die in Belgien niedergelassen sind und mindestens eine der in den Anhängen des Gesetzes aufgeführten Dienstleistungen innerhalb der Europäischen Union erbringen. Das Größenkriterium bedeutet, dass die Einrichtung mindestens 50 Vollzeitbeschäftigte oder einen Jahresumsatz (oder eine Jahresbilanzsumme) von mehr als 10 Millionen Euro haben muss. Die Zahl der betroffenen Sektoren hat sich damit von 7 auf 18 deutlich erhöht.

Meldung von Vorfällen und Registrierung sind die ersten Schritte

Ab dem 18. Oktober müssen die Organisationen dem CCB innerhalb von 24 Stunden bedeutende Vorfälle melden, gefolgt von weiteren Informationen innerhalb von 72 Stunden und einem Abschlussbericht innerhalb von 30 Tagen.

Darüber hinaus müssen sich alle NIS2-Unternehmen und -Organisationen bis zum 18. März 2025 über einen gesetzlichen Vertreter auf dem Portal atwork.safeonweb.be registrieren. Die Registrierung erfordert Informationen über die Organisation, einschließlich Kontaktperson, Branche und Größe. Nach der

Registrierung erhalten die Unternehmen Zugang zu zusätzlichen Diensten, die dabei helfen, Cyber-Bedrohungen zu erkennen und abzuschwächen, die auf das Netzwerk und den Bereich des jeweiligen Unternehmens zugeschnitten sind.

CyberFundamentals framework: ein schrittweiser Ansatz

Alle Unternehmen müssen die notwendigen Maßnahmen ergreifen, um ihre Cybersicherheit zu erhöhen. Zu diesem Zweck hat das CCB den CyberFundamentals-Rahmen bereitgestellt. Der CCB unterstützt Organisationen mit einer Risikobewertung, die es jeder Organisation ermöglicht, das angemessene Niveau der CyberFundamentals zu bestimmen. Dieses innovative Rahmenwerk enthält schrittweise zusätzliche Maßnahmen für jede Sicherheitsstufe, die auf internationalen Cybersicherheitsstandards und Erkenntnissen aus Tausenden von Vorfällen basieren.

Der letzte Teil: die Zertifizierung

"Wesentliche Einrichtungen müssen sich auch regelmäßigen Bewertungen auf der Grundlage der CyberFundamentals oder der ISO 27001-Norm unterziehen", sagt Johan Klykens, Direktor für Zertifizierung beim Centre for Cybersecurity Belgium (CCB). "Diese Zertifizierung bietet Unternehmen eine klare Methode, um nachzuweisen, dass sie ihre Verantwortung in Bezug auf die Cybersicherheit wahrgenommen haben."

In Fällen, in denen IT-Dienste ausgelagert werden, bleibt die rechtliche Verantwortung jedoch bei der Organisation selbst. Es ist von entscheidender Bedeutung, von den Anbietern Garantien und Zertifizierungen zu verlangen, was über den CyberFundamentals-Rahmen möglich ist. Darüber hinaus empfiehlt der CCB, die Cybersicherheitsanforderungen der wichtigsten IT-Lieferanten in die maßgeschneiderte Bewertung der Organisation aufzunehmen.

Es versteht sich von selbst, dass der CCB alle Organisationen, die nicht unter die NIS2-Gesetzgebung fallen, dazu ermutigt, mit Hilfe der CyberFundamentals an der Cybersicherheit zu arbeiten. Nur weil eine Organisation nicht als Einrichtung gilt, die unter die NIS2-Gesetzgebung fällt, bedeutet dies nicht, dass sie die Anforderungen der Gesetzgebung ignorieren kann. In der Praxis werden viele Organisationen die Anforderungen erfüllen müssen, da sie Dienstleistungen für NIS2-Stellen erbringen.

Alle Ressourcen

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

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

© 2024 - news.belgium.be