22 Aug. 2025 -06:00

Weniger als die Hälfte der belgischen Unternehmen nutzt die grundlegendsten Sicherheitsmaßnahmen!

Trotz eines wachsenden Bewusstseins für Cyberbedrohungen zeigt eine aktuelle Studie des Zentrum für Cybersicherheit Belgien (ZCB), dass belgische Unternehmen Zwei-Faktor-Authentifizierung (2FA) oder Multi-Faktor-Authentifizierung (MFA) bei externen Verbindungen nur unzureichend einsetzen. Während 70% der befragten Unternehmen angeben, dass sie es für etwas bis sehr wahrscheinlich halten, bald Ziel von Cyberkriminellen zu werden, haben nur 46,4% tatsächlich 2FA implementiert.

Dies geht aus einer Umfrage hervor, die das ZCB im Juli 2025 unter 250 belgischen Unternehmen durchgeführt hat. Die Ergebnisse zeigen einen auffälligen Kontrast zwischen der wahrgenommenen Bedrohung und den getroffenen Maßnahmen. „*Diese Zahlen und die Anzahl der Vorfälle sind sehr beunruhigend*“, sagt Miguel De Bruycker, Generaldirektor des ZCB. „*Bei etwa der Hälfte unserer Incident-Response-Einsätze stellen wir fest, dass 2FA oder MFA nicht oder nur teilweise eingesetzt werden. In einer digitalen Umgebung, in der Passwort-Hacking von 58% der Unternehmen als reale Bedrohung angesehen wird, sollte 2FA eine absolute Mindestmaßnahme sein*.“

Täglich Opfer durch gestohlene Anmeldedaten und fehlende 2FA

Täglich wird mindestens ein belgisches Unternehmen Opfer eines Cyberangriffs. Der rote Faden bei diesen Vorfällen ist das Durchsickern von Anmeldedaten, beispielsweise durch Phishing, und das Fehlen einer korrekten Zwei-Faktor-Authentifizierung.

> “Installieren Sie 2FA sofort auf allen externen Verbindungen und für alle Benutzer”
>
> Miguel De Bruycker
> Generaldirektor des Zentrum für Cybersicherheit Belgien (ZCB)

Bei Vorfällen wird auch häufig festgestellt, dass 2FA nicht für alle vorgesehen ist. Kürzlich wurden massenhaft Daten gestohlen, weil die IT-Administratoren ein separates VPN zu den Servern ohne 2FA eingerichtet hatten, während alle anderen Mitarbeiter diese verwenden mussten. Daher sind ein Bewusstsein und Kontrollen durch die oberste Führungsebene erforderlich.

2FA: einfach, effektiv, aber noch zu wenig eingesetzt

Die Zwei-Faktor-Authentifizierung bietet eine zweite Sicherheitsebene zusätzlich zum herkömmlichen Passwort. Selbst wenn dieses Passwort in die falschen Hände gerät, bleibt der Zugriff auf das System ohne das zweite Authentifizierungsmittel (z. B. eine App oder einen Token) gesperrt. Dennoch hinkt die Implementierung im Vergleich zu anderen grundlegenden Maßnahmen hinterher:

- Antivirensoftware: 89,6%
- Backups: 86,4%
- Firewall-Schutz: 77%
- Zwei-Faktor-Authentifizierung: 46,4%

Es ist falsch zu glauben, dass es keine große Rolle spielt! 2FA ist keine absolute Sicherheit, aber sie macht einen enormen Unterschied. Mehr als 80% der aktuellen Vorfälle hätten durch die korrekte Implementierung dieser einen, wichtigsten Maßnahme vermieden werden können.

Vom Bewusstsein zur Tat
Die Implementierung von 2FA muss weder komplex noch teuer sein. Viele beliebte Anwendungen und Cloud-Dienste bieten diese Option standardmäßig an. Unternehmen, die 2FA noch nicht eingeführt haben, gehen unnötige Risiken ein. Das ZCB fordert Unternehmen daher auf:

- 2FA für alle von außen zugänglichen Konten verbindlich einzuführen, insbesondere für E-Mail, Cloud-Plattformen, VPNs und Administrator-Schnittstellen.
- Nutzen Sie unsere CyberFundamentals für eine starke Cyberabwehr.
- Mitarbeiter aktiv für sicheres Einloggen zu sensibilisieren.

Weitere Informationen, praktische Leitfäden und Unterstützung finden Unternehmen unter ccb.belgium.be

Quelle

- Umfrage unter 250 belgischen Unternehmen, durchgeführt vom Zentrum für Cybersicherheit Belgien, Juli 2025.
- Safeonweb AT Work

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

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

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