22 Aug 2025 -06:00

Less than half of Belgian companies use the most basic security measures!

Despite growing awareness of cyber threats, recent research by the Centre for Cybersecurity Belgium (CCB) shows that Belgian companies are not making sufficient use of two-factor authentication (2FA) or multi-factor authentication (MFA) on external connections. While 70% of the organisations surveyed say they consider it somewhat to very likely that they will soon be targeted by cybercriminals, only 46.4% have actually implemented 2FA.

A survey of 250 Belgian companies conducted by the CCB in July 2025 clearly demonstrates this. The results show a striking contrast between the perceived threat and the measures taken. “*These figures and the number of incidents are very worrying,*" says Miguel De Bruycker, Director-General at the CCB. “*In about half of our Incident Response Interventions, we find that 2FA or MFA is not or only partially in use. In a digital environment where password hacking is seen as a real threat by 58% of companies, 2FA should be an absolute minimum measure*.”

Daily victims due to leaked login details and incorrect 2FA

Every day, at least one Belgian company falls victim to a cyber attack. The common thread in these incidents is the leakage of login details through phishing, for example, and the lack of proper two-step verification.

> "Install 2FA immediately on all external connections and for everyone"
>
> Miguel De Bruycker
> Director-General at the Centre for Cybersecurity Belgium (CCB)

In incidents, it is also often found that 2FA is not provided for everyone. Recently, massive amounts of data were stolen because IT administrators had set up a separate VPN to the servers without 2FA, while all other employees were required to use it. Awareness and control by top management is therefore essential.

2FA: simple, effective, but still underused
Two-step verification provides a second layer of security on top of the traditional password. Even if that password falls into the wrong hands, access to the system remains blocked without the second means of authentication (such as an app or token). Nevertheless, its implementation lags behind other basic measures:

- Antivirus software: 89.6%
- Backups: 86.4%
- Firewall protection: 77%
- Two-step verification: 46.4%

It is wrong to think that it does not matter much! 2FA is not absolute security, but it makes a huge difference. More than 80% of current incidents could have been avoided by correctly implementing this one, most important measure.

From awareness to action
Implementing 2FA does not have to be complex or expensive. Many popular applications and cloud services offer this option as standard. Organisations that have not yet implemented 2FA are taking unnecessary risks. The CCB therefore calls on companies to:

- Mandatory implementation of 2FA on all accounts that are accessible from outside the organisation, especially for email, cloud platforms, VPNs and administrator interfaces.
- Use our CyberFundamentals for strong cyber defence
- Actively raise employee awareness about secure login.

For more information, practical guides and support, companies can visit: ccb.belgium.be

Sources

- Survey of 250 Belgian companies conducted by the Centre for Cybersecurity Belgium, July 2025.
- Safeonweb AT Work

Centre for Cyber Security Belgium
Rue de la Loi 18
1000 Brussels
Belgium
http://www.ccb.belgium.be

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

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