22 aug 2025 -06:00

Minder dan de helft van de Belgische bedrijven gebruikt de meest elementaire beveiligingsmaatregel!

Ondanks een groeiend bewustzijn over cyberdreigingen blijkt uit recent onderzoek van het Centrum for Cybersecurity België (CCB) dat Belgische bedrijven onvoldoende gebruik maken van tweestapsverificatie (2FA) of Multifactor Authentication (MFA) op externe verbindingen. Terwijl 70% van de bevraagde organisaties aangeeft het enigszins tot zeer waarschijnlijk te achten dat ze binnenkort het doelwit worden van cybercriminelen, heeft slechts 46,4% effectief 2FA geïmplementeerd.

Dat blijkt uit een bevraging van 250 Belgische bedrijven die het CCB in juli 2025 uitvoerde. De resultaten tonen een opvallend contrast tussen de waargenomen dreiging en de genomen maatregelen. “Deze cijfers en het aantal incidenten zijn zeer verontrustend” zegt Miguel De Bruycker, directeur-generaal bij het CCB. “Bij ongeveer de helft van onze Incident Respons Interventies vernemen wij dat 2FA of MFA niet of slechts gedeeltelijk in gebruik is. In een digitale omgeving waar wachtwoordhacking door 58% van de bedrijven als een reële bedreiging wordt gezien, zou 2FA een absolute minimummaatregel moeten zijn.”

Dagelijks slachtoffers door gelekte logingegevens en geen correcte 2FA

Dagelijks wordt minstens één Belgisch bedrijf het slachtoffer van een cyberaanval. De rode draad bij deze incidenten is het lekken van logingegevens door bijvoorbeeld phishing en het ontbreken van een correcte tweestapsverificatie.

> "Installeer onmiddellijk 2FA op alle externe verbindingen
>
> én voor iedereen"
>
> Miguel De Bruycker
> Directeur-generaal bij het Centrum for Cybersecurity België(CCB)

Bij incidenten wordt ook vaak vastgesteld dat 2FA niet voor iedereen wordt voorzien. Recentelijk werden massaal gegevens gestolen omdat de ICT-beheerders een afzonderlijke VPN naar de servers hadden opgezet zonder 2FA, terwijl alle andere medewerkers het wel moesten gebruiken. Een bewustzijn én controle door het topmanagement is dus noodzakelijk.

2FA: eenvoudig, doeltreffend, maar nog te weinig toegepast
Tweestapsverificatie biedt een tweede beveiligingslaag bovenop het traditionele wachtwoord. Zelfs als dat

wachtwoord in verkeerde handen valt, blijft toegang tot het systeem geblokkeerd zonder het tweede authenticatiemiddel (zoals een app of token). Toch blijft de implementatie ervan achter in vergelijking met andere basismaatregelen:

- Antivirussoftware: 89,6%
- Back-ups: 86,4%
- Firewallbescherming: 77%
- Tweestapsverificatie: 46,4%

Het is onjuist te denken dat het niet veel uitmaakt! 2FA is geen absolute zekerheid, maar het maakt een enorm verschil. Meer dan 80% van de huidige incidenten had vermeden kunnen worden door een correct implementatie van deze ene, meest belangrijke maatregel.

Van bewustzijn naar actie
Het implementeren van 2FA hoeft niet complex of duur te zijn. Veel populaire toepassingen en clouddiensten bieden deze optie standaard aan. Organisaties die 2FA nog niet invoerden, lopen onnodig risico. Het CCB roept bedrijven dan ook op om:

- 2FA verplicht in te voeren op alle accounts die van buitenaf bereikbaar zijn, zeker voor e-mail, cloudplatformen, VPN’s en beheerdersinterfaces.
- Gebruik te maken van onze CyberFundamentals voor een sertke cyberverdediging
- Werknemers actief te sensibiliseren over veilig inloggen.

Voor meer informatie, praktische gidsen en ondersteuning kunnen bedrijven terecht op ccb.belgium.be

Bron

- Survey bij 250 Belgische bedrijven uitgevoerd door het Centrum voor Cybersecurity België, juli 2025.
- Safeonweb AT Work

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

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

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