

08 jun 2023 -08:00

Het Centrum voor Cybersecurity België waarschuwt: neem nu de belangrijkste maatregel tegen cyberaanvallen. Installeer tweestapsverificatie (2FA) op alle externe verbindingen

Hou hackers buiten!

Het Centrum voor Cybersecurity België (CCB) adviseert alle bedrijven en organisaties in ons land om zo snel als mogelijk tweestapsverificatie (2FA) te activeren op alle externe verbindingen. Deze maatregel is meestal eenvoudig en goedkoop te implementeren. Een kleine inspanning van de organisatie en de medewerkers die een enorm verschil maakt voor de cyberveiligheid.

Dagelijks wordt er minstens één bedrijf in ons land het slachtoffer van een ransomware-aanval of afpersing na diefstal van gevoelige informatie. In het eerste kwartaal van 2023 deden al 27 organisaties een melding bij ons over een ransomware-aanval. Met de regelmaat van de klok worden ziekenhuizen en andere zorginstellingen slachtoffer met grote gevolgen voor de patiëntenzorg. Een half jaar na de cyberaanval op de stad Antwerpen is de schade nog steeds niet volledig hersteld.

“ De impact van een cyberaanval is vaak zeer groot. Het bedrijf dat slachtoffer wordt, kan niet normaal verder functioneren, verliest cruciale informatie, lijdt belangrijke reputatieschade en ziet de kosten stevig oplopen. ”

Miguel De Bruycker
Directeur-generaal, Centrum voor Cybersecurity België

We zijn niet weerloos tegen ransomware: installeer vandaag nog tweestapsverificatie

Geen enkele sector blijft gespaard, nochtans kunnen ransomware-aanvallen vaak vermeden worden. Uit ons onderzoek van deze incidenten blijkt dat cybercriminelen vaak gebruik maken van gestolen logingegevens om hun aanval in te zetten. De logingegevens worden gestolen via phishingberichten of met behulp van computervirussen die wachtwoorden stelen in de browser.

Een groot deel van deze cyberaanvallen kon voorkomen worden door gebruik te maken van tweestapsverificatie (2FA) of multifactorauthenticatie (MFA) op alle verbindingen van buiten het bedrijf of

de organisatie. Hierbij moet een medewerker die zich van buiten het bedrijf verbindt met het bedrijfsnetwerk of bedrijfsmailbox zich in minstens 2 stappen aanmelden: bijvoorbeeld met een wachtwoord en een code op de smartphone. Gebruik voor externe toegang altijd een combinatie van minstens 2 elementen uit iets dat je weet (bv. een wachtwoord), iets dat je bent (bv. gezichtsherkenning) of iets dat je hebt (bv. een smartphone / telefoonnummer).

Belangrijk en niet moeilijk

Laat tweestapsverificatie of MFA de eerste stap zijn naar een veiligere omgeving, gevolgd door andere maatregelen zoals snel security updates uitvoeren en periodiek offline back-ups maken. Begin vandaag met de eerste stap.

[Hoe tweestapsverificatie implementeren?](#)

Laten we samen de strijd aangaan tegen de cybercriminaliteit!

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

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

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