01 okt 2020 -11:00

Wachtwoorden zijn niet meer van deze tijd. Gebruik tweestapsverificatie (2FA)

Wachtwoorden maken ons □□□□! Wachtwoorden bedenken, onthouden en gebruiken is vervelend, frustrerend, tijdrovend en ook niet voor 100% veilig, want zelfs het sterkste wachtwoord kan gestolen en misbruikt worden. Daarom voert het Centrum voor Cybersecurity België (CCB) dit jaar campagne om een betere beveiliging van accounts te promoten!

In het kader van de *European Cyber Security Month* lanceren het Centrum voor Cybersecurity België (CCB) en de Cyber Security Coalition voor de zesde keer samen een sensibiliseringscampagne rond cyberveiligheid. Dit jaar willen we de internetgebruiker aanmoedigen om accounts sterk te beveiligen met tweestapsverificatie.

Online accounts (bv. e-mail, sociale netwerken, internetbankieren en online webwinkels) worden meestal beveiligd met een gebruikersnaam en een wachtwoord. Gebruikers kiezen helaas vaak wachtwoorden die gemakkelijk te onthouden zijn en ze gebruiken bovendien voor verschillende accounts hetzelfde wachtwoord. Dit maakt het eenvoudig voor hackers om toegang te krijgen tot die accounts. Als een buitenstaander toegang krijgt tot een account, kan die zich voordoen als de eigenaar en dit misbruiken.

> "Daarom raden wij gebruikers aan om zoveel mogelijk tweestapsverificatie in te stellen, verschillende wachtwoorden te gebruiken en deze te laten beheren door een online wachtwoordkluis. Ikzelf ken maar één wachtwoord! Dat is het wachtwoord van mijn wachtwoordkluis.In die kluis worden al mijn wachtwoorden bewaard.De wachtwoordkluis maakte bovendien voor al mijn accounts sterke wachtwoorden van meer dan 20 tekens, die ik zelf nooit hoef te kennen, laat staan onthouden."
>
> Miguel De Bruycker
> Directeur Centrum voor Cybersecurity België

> "Ook in een professionele context raden wij aan om van tweestapsverificatie de regel te maken voor medewerkers, zodat cybercriminelen de interne netwerken niet door een eenvoudige phishingaanval kunnen binnen dringen"

Jan Deblauwe
Voorzitter Cyber Security Coalition Belgium

In cijfers

- Zwakke wachtwoorden waren in 2019 verantwoordelijk voor zo'n dertig procent van alle ransomware-infecties. (https://www.precisesecurity.com/articles/weak-passwords-caused-30-of-ransomware-infections-in-2019/)
- 1 seconde: is de tijd nodig om een wachtwoord met 4 tekens te kraken
- 1 week: is de tijd nodig om een sterk wachtwoord met 10 tekens te kraken.
- Om een wachtwoord met 13 tekens te kraken heb je als hacker met de huidige technologie vele eeuwen tijd nodig. Daarom proberen hackers wachtwoorden te stelen… Of ze via een smoes te achterhalen (phishing, smishing, scam…)(https://www.grc.com/haystack.htm)
- 15% gebruikt hetzelfde wachtwoord voor elke account en 53% gebruikt enkele wachtwoorden. Slechts 32% gebruikt veel verschillende wachtwoorden. (Digitale Gezondheidsindex, nov 2019)

Resultaten eigen survey over het gebruik van tweestapsverificatie, augustus 2020

- 30% maakt gebruik van een wachtwoordkluis en 40% gebruikt tweestapsverificatie waar mogelijk.
- 33% heeft nog nooit gehoord over tweestapsverificatie of 2FA
- Mensen die tweestapsverificatie wel kennen, gebruiken het vaak toch niet omdat ze niet weten dat de mogelijkheid bestaat. Bv. 57% van de Facebookgebruikers weet niet dat tweestapsverificatie mogelijk is of hoe dat moet op Facebook. Hetzelfde geldt voor gebruikers van Twitter en Instagram.
- De meest gebruikte methode voor tweestapsverificatie is en sms-bericht met code (89%) gevolgd door

een authenticatie-App zoals bv. Itsme of Google Authenticator (80%) en een token (70%) of biometrische methode (digitale vingerafdruk of gezichtsherkenning) (56%)

Vergeet dat wachtwoord!

We vinden het frustrerend om wachtwoorden te gebruiken. Je moet steeds nieuwe wachtwoorden zoeken, ze moeten van alles en nog wat bevatten (speciale tekens, hoofdletters, kleine letters, cijfers) en ze moeten lang zijn. Zo lang dat je steevast moet herbeginnen door een typefoutje. En ga zo maar verder. Zucht.

De meeste internetgebruikers beseffen wel dat een kort en eenvoudig wachtwoord niet pluis is, toch merken we dat zwakke wachtwoorden nog steeds gebruikt worden. 123456, azerty, wachtwoord, een voornaam, een lievelingsploeg, ‘bolleke’ of ‘sloeber’, het is maar een kleine greep uit de top 30 van meest gebruikte wachtwoorden in België. Hoe korter en eenvoudiger een wachtwoord is, hoe sneller het zelfs door beginnende hacker gekraakt kan worden.

Top 30 meest gebruikte wachtwoorden in België (2015-2020)

123456	computer
azerty	thomas
123456789	mercedes
12345	charlotte
azertyuiop	standard
wachtwoord	vergeten
abc123	unknown
pokemon	nicolas
azerty123	lol123
password	nathalie
voetbal	snoopy
12345678	motdepasse

anderlecht	bolleke
sloeber	1234567890
loulou	isabelle

BRON: Scattered Secrets

> "Wachtwoorden zijn de sleutels van je virtuele woning die zelfs naar je kluis kunnen leiden. Bewaar ze dus zorgvuldig"
>
> Olivier Bogaert
> Federal Computer Crime Unit

Frustrerend, en ook niet helemaal veilig

Sterke wachtwoorden gebruiken is absoluut een must, maar ook dan kan je nog niet op beide oren slapen. Ook sterke wachtwoorden kunnen gestolen worden:

- Criminelen proberen je wachtwoord te stelen door je om de tuin te leiden met een phishingmail. Op die manier proberen ze je bijvoorbeeld te overhalen om je wachtwoord in te voeren in een vervalste website waardoor ze je wachtwoord gewoon kunnen lezen.
- Datalekken komen ook voor. Het kan gebeuren dat een platform dat jij gebruikt, zoals bv. LinkedIn of Facebook gehackt wordt en dat alle gegevens van de gebruikers worden gestolen, waaronder ook de wachtwoorden.

Soms maken we het de hackers wel heel gemakkelijk:

- je wachtwoorden staan op een Post-itje dat aan je scherm hangt,
- je geeft je wachtwoorden prijs aan de telefoon, als je opgebeld wordt door een zogezegde medewerker van Microsoft,
- je hebt je gegevens ingegeven om deel te nemen aan één of andere prijsvraag of wedstrijd,
- je bewaart je wachtwoorden in een document op je computer met de naam ‘wachtwoorden’

- enz...

Sterke wachtwoorden gebruiken is absoluut belangrijk, maar wij raden aan om er nog een beveiligingslaag boven op te doen: namelijk tweestapsverificatie (2FA).

Tweestapsverificatie (2FA): de oplossing!

Tweestapsverificatie of 2FA is een eenvoudige oplossing om je gegevens nog beter te beschermen.

Om toegang te krijgen tot je account moet je bewijzen dat je bent wie je beweert te zijn. Dat kan op drie verschillende manieren, of factoren:

- met iets dat jij alleen weet (jouw wachtwoord of pincode);
- met iets dat jij alleen hebt (jouw telefoon of token);
- met iets dat jij bent (jouw vingerafdruk, gelaat, iris...).

Meestal gebruik je één van deze factoren om te bewijzen wie je bent, maar het is beter om 2 of meer factoren te gebruiken: dit is twee- of meerstapsverificatie (2FA of MFA). Je gebruikt dan bv. een wachtwoord en je laat daar bovenop ook een code naar je GSM sturen, of je gebruikt je vingerafdruk en een code om toegang te krijgen.

> "Niets is zo frustrerend als hacker om na de euforie van het kraken van een wachtwoord vast te stellen dat het doelwit 2FA heeft geïnstalleerd"
>
> Inti De Ceukelaire
> Ethical Hacker

Samen campagne voeren!

Tijdens de campagnemaand oktober willen we de aandacht vestigen op het thema via radiospotjes,

filmpjes op social media, banners en andere campagnematerialen. Op de campagnewebsite https://campagne.safeonweb.be/nl staan nuttige tips en informatie. Je vindt er ook de digitale gezondheidsindex terug, zodat je je cyber security kennis kan testen. Al het campagnemateriaal kan je downloaden op https://safeonweb.be/nl/campagnemateriaal

> "Wij zijn heel dankbaar voor al onze partners die mee hun schouders zetten onder de campagneboodschap. Federale overheidsdiensten, academische instellingen, grote en kleine bedrijven, maar ook vzw's en andere organisaties ondersteunen de campagne. Ook dit jaar zullen uiteindelijk meer dan 500 partners het campagnemateriaal helpen verspreiden."
>
> Phédra Clouner
> Adjunct-Directrice, Centrum voor Cybersecurity België

Centrum voor Cyber Security België
Wetstraat 16
1000 Brussel
België
http://www.ccb.belgium.be

Andries Bomans
Communicatieverantwoordelijke
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien - Eggers
Communicatieverantwoordelijke
+32 485 76 53 36
katrien.eggers@cert.be