Twee-factor authenticatie *(afgekort: 2FA)*

Wat is het?

- Authenticatie is het aantonen/vaststellen dat je de persoon bent die je aangeeft te zijn.
- Authenticatie kent drie vormen: iets wat je weet (bijvoorbeeld een wachtwoord), iets wat je hebt (bijvoorbeeld een app/token met wijzigende code) of met iets wat je bent (bijvoorbeeld je gezicht of vingerafdruk).
- 2FA geeft aan dat je je identiteit aantoont met een combinatie van twee vormen (zie punt hierboven), bijvoorbeeld een wachtwoord en een code uit een app.
- Door twee vormen te combineren, is de kans zeer sterk verkleind dat er (grote) schade optreedt, als een van de middelen (zoals je wachtwoord) bekend is bij een aanvaller.
- Twee keer hetzelfde type authenticatie (2x een wachtwoord) is geen 2FA.

Belang voor Nederland

- Wachtwoorden zijn door o.a. datalekken en hacks steeds minder zeker. Door 2FA te implementeren, is de kans op het misbruiken van een account sterk verkleind.
- 2FA is bij alle belangrijke diensten (zoals bij social media, cloud, overheid, werkplekken, en het thuiswerken, etc.) standaard aanbevolen (maar niet verplicht). Het is alleen nog niet algemeen in gebruik als het niet wordt afgedwongen.
- Veilig en integer authentiseren is essentieel voor het gebruik van digitale diensten.

Gevolgen bij misbruik

- Als een wachtwoord gehackt of op andere wijze bekend is bij een aanvaller, dan kan een aanvaller zich voordoen als een ander persoon.
- Met 2FA heeft o.a. Google voor haar eigen personeel aangetoond dat de schade door gehackte wachtwoorden praktisch volledig is verdwenen.
- Sommige 2FA, zoals een SMS, verlopen via kanalen die zelf ook minder veilig zijn. Hierdoor is de zekerheid van een tweede factor verminderd.
- Malware wordt ook steeds geavanceerder en er zijn gevallen waarin men 2FA weet af te vangen/vervalsen. Bijvoorbeeld op smartphones met malware (waar zowel de bankieren-app op draait als de sms binnenkomt).

Is misbruik al eens voorgekomen?

- Ja, wachtwoorden worden regelmatig gestolen van gehackte organisaties en kunnen gekocht worden.
- Ja, er is malware voor Android telefoons die ook 2FA kan omzeilen, gericht op bankieren (bijvoorbeeld TrickBot en Cerberus).
- Via social engineering worden mensen overgehaald de codes van een tweede factor aan een aanvaller te sturen, bijv. in 2020 met de Whatsapp beveiligingscode.

Cybersecurity specifieke relevante nationale wetgeving of andere richtlijnen

- Voor de overheid: de BIO: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/kaders-voor-informatieveiligheid/baseline-informatiebeveiliging-overheid/
- Voor Aanbieders van Essentiele Diensten, de Wbni: https://wetten.overheid.nl/BWBR0041515/2021-08-01

Veilig Internetten over 2FA (video)
https://veiliginternetten.nl/inloggen-in-twee-stappen

Veilig Internetten – info over 2FA
https://veiliginternetten.nl/uitlegvideos/in-twee-stappen-inloggen-tweestapsverificatie/detail/

NCSC aanbeveling over authenticatie
https://www.ncsc.nl/onderwerpen/authenticatie

Wat is 2FA en waarom is het belangrijk?
https://www.youtube.com/watch?v=ow0UbVo4yp8