INFORMATIE
BEVEILIGINGS
DIENST

VNG Realisatie

# 2 - Factor Authenticatie – 2FA

INFORMATIE
BEVEILIGINGS
DIENST

# De gastheer van vandaag

VNG Realisatie

Jule Hintzbergen

INFORMATIE BEVEILIGINGS DIENST

# Doel Webinar

VNG Realisatie

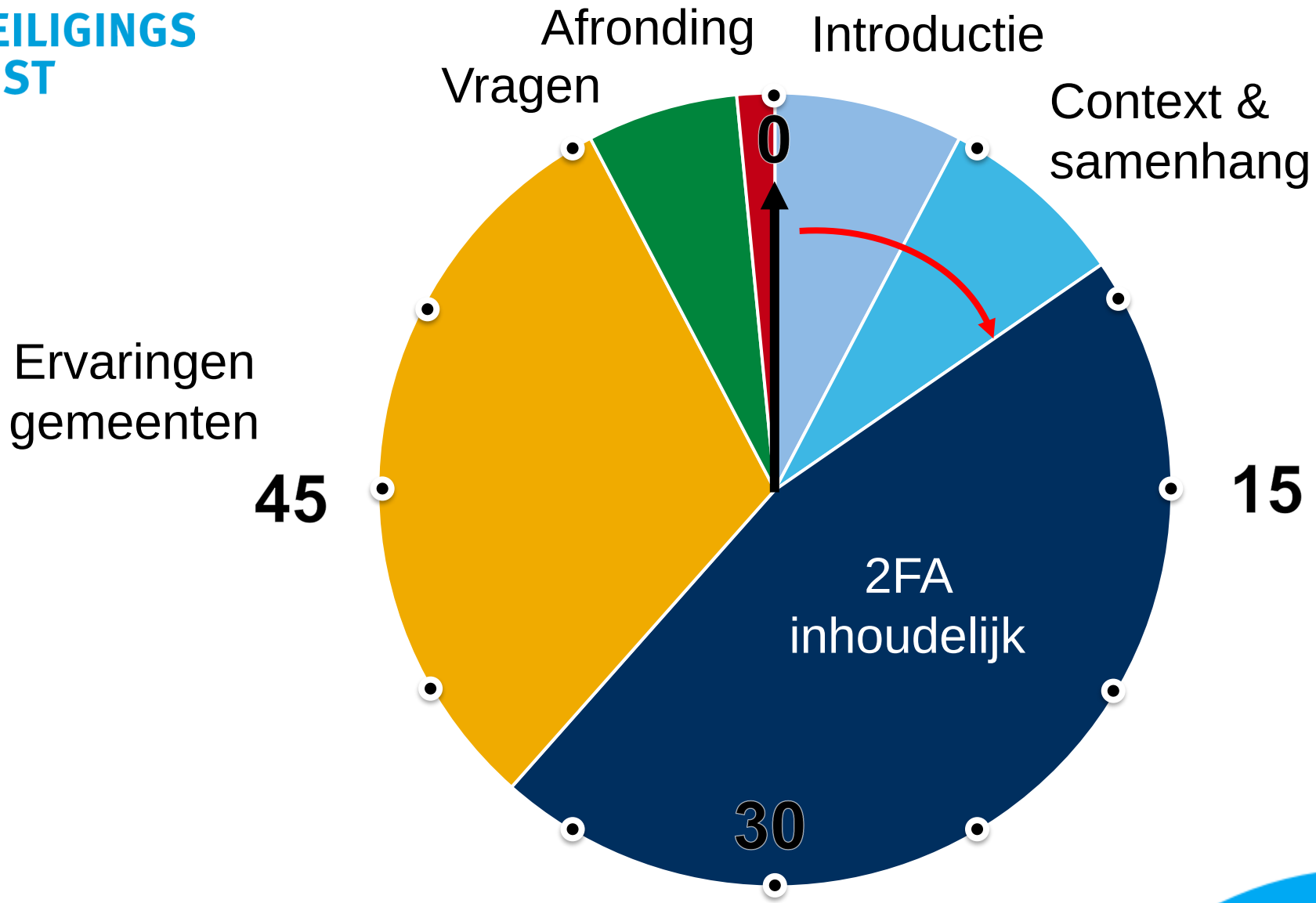
## Na het volgen van deze webinar:

- Is er beter inzicht in het IAA Concept
- Is er meer duidelijkheid over het onderwerp 2FA
- Is er kennis gedeeld, ook door andere deelnemers
- Kun je zelf aan de slag met 2FA

# Webinar 2-Factor Authenticatie (60 min)

INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie



INFORMATIE BEVEILIGINGS DIENST

# Inhoud

VNG Realisatie

- Waarom
- IAA Concept
- Het waarom
- Techniek
- Ervaringen
- Vragen
- Afronding

INFORMATIE BEVEILIGINGS DIENST

# Waarom?

VNG Realisatie

# 10.199.352.448

Heeft iemand enig idee wat dit is?

Dit zijn de aantallen gevonden credentials in Haveibeenpwned (stand van ongeveer een week geleden).

(En op het Darkweb is het nog eenvoudiger, om wachtwoorden te vinden)

INFORMATIE BEVEILIGINGS DIENST

# Waarom?

VNG Realisatie

# 1.200.000

Heeft iemand enig idee wat dit is?

Dit zijn aantallen gecompromitteerde accounts op O365 in de maand januari 2020

-

Gemiddeld wordt 0,5% van de accounts gehackt

Bij 99,9% van deze accounts staat MFA uit

Bron: https://www.windowscentral.com/microsoft-999-people-get-hacked-one-ridiculous-reason
https://www.zdnet.com/article/microsoft-99-9-of-compromised-accounts-did-not-use-multi-factor-authentication

INFORMATIE BEVEILIGINGS DIENST

# BIO Eisen

VNG Realisatie

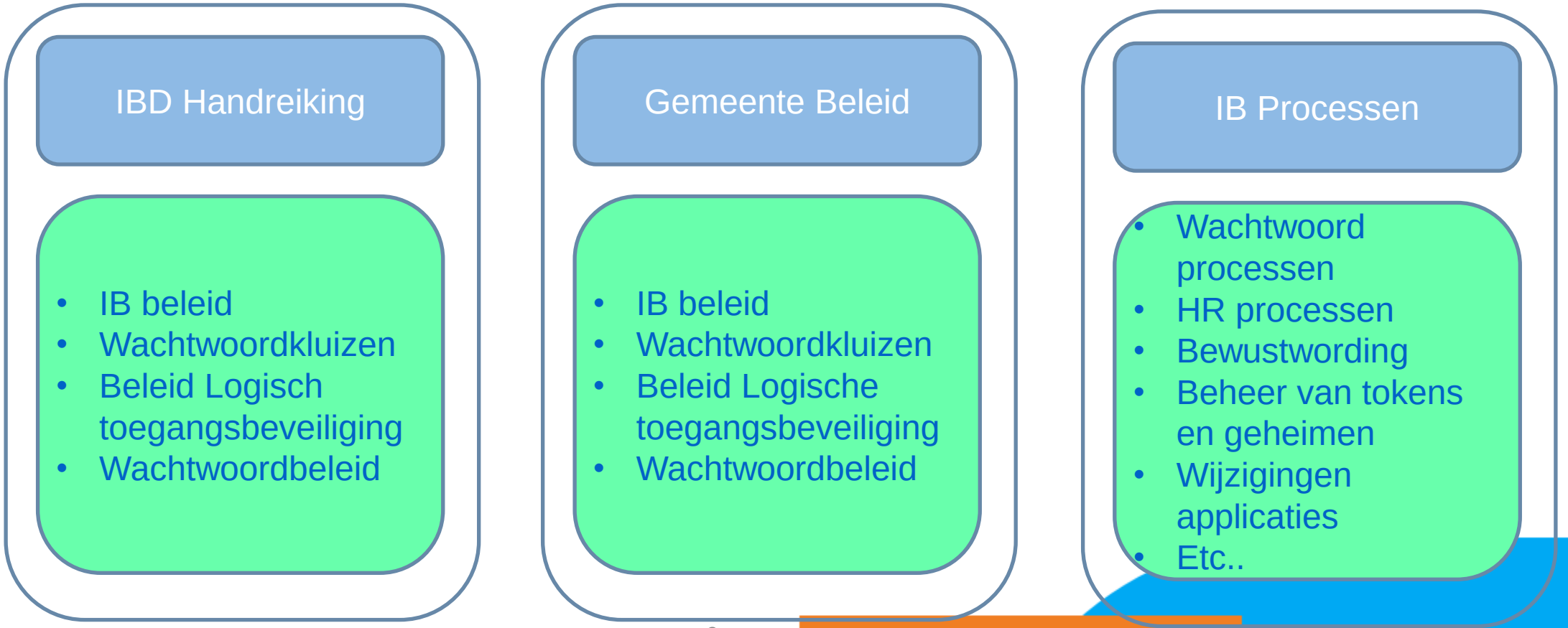
| | | | |
|---|---|---|---|
| 9.4.2 | 1 | Beveiligde inlogprocedures<br><br>Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure. | Proceseigenaar<br><br>Dienstenleverancier |
| 9.4.2.1 | 1 | **Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie** | |

INFORMATIE BEVEILIGINGS DIENST

# De handreiking

VNG Realisatie

De handreiking gaat in op diverse aspecten van 2FA, maar er zijn ook relaties met:



INFORMATIE BEVEILIGINGS DIENST

# IAA Concept

VNG Realisatie

Het IAA concept is de basis om te begrijpen als het om toegang tot systemen gaat, het gaat hier om:

INFORMATIE BEVEILIGINGS DIENST

# Wat is 1FA

VNG Realisatie

Factor 1: iets wat je weet – wachtwoord

**In het IAA concept met alleen een wachtwoord zit wel een zwakheid!**

- Wachtwoorden kunnen worden gestolen, gekraakt, gedeeld etc.

Dus hoe maak je dit proces sterker?

INFORMATIE BEVEILIGINGS DIENST

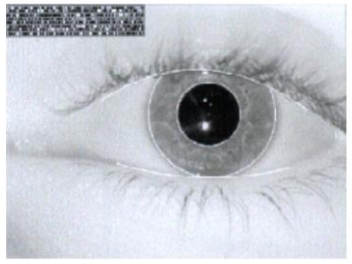
# Wat is 2FA / MFA?

VNG Realisatie

Voeg een extra factor toe aan de authenticatie stap!

- Factor 2: iets wat je hebt – een token, een app, een key fob


- Factor 3: iets wat je bent – Biometrie (kan meerdere soorten zijn)



INFORMATIE BEVEILIGINGS DIENST

# Waarom 2FA?

VNG Realisatie

Omdat het in de BIO staat, of omdat je dit gewoon wilt?

Risico's van alleen wachtwoorden:

- Stelen van identiteiten
- Stelen van wachtwoorden
- Je voordoen als een ander
- Hacken / ransomware en andere aanvalspatronen

Dus:

- Extra drempel inbouwen naast gebruikersnaam en wachtwoord

INFORMATIE BEVEILIGINGS DIENST

# Soorten

VNG Realisatie

Er zijn vele soorten oplossingen om 2FA te implementeren, deze zijn:

- Tokens 

Een token die een code geeft of zelf de code is (FIDO)
- Apps 
Een app die een code geeft
- SMS 
een code die als SMS ontvangen wordt

INFORMATIE BEVEILIGINGS DIENST

# Tokens

VNG Realisatie

- Het zijn op zichzelf staande, niet-koppelbare apparaten, het is niet mogelijk om van buiten toegang te krijgen;
- De SIM kaart kan niet gestolen worden, want die zit er niet in;
- De gegevens van de code generator zijn ongevoelig voor een aanval waarbij een aanvaller de codes onderschept in het geheugen van de telefoon of computer (man-in-the-middle (MITM)-aanval)).
- De batterijen van de tokens gaan jarenlang mee, meestal langer dan de levensduur van de codegenerator.
- Ze hebben geen mobiel netwerksignaal of roaming nodig om te werken zoals bij SMS.

INFORMATIE BEVEILIGINGS DIENST

# Soorten - Tokens

VNG Realisatie

- Er zijn vele soorten tokens op de markt, contactloze tokens en connected tokens

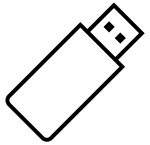
Contactloze:


- Fysiek token
- Bestaat met voorgeïnstalleerde sleutels en zelf te installeren sleutels

2 varianten:

- Toont periodiek een nieuwe code (TOTP)
- Genereerd een code na invoer van een PIN, is langer geldig (vergelijk tancode)

Connected:



- Op basis van de U2F standaard (FIDO)
- Fysiek token
- USB koppeling
- Ook varianten met bluetooth/NFC en biometrie
- Bevatten af fabriek sleutelmateriaal

INFORMATIE BEVEILIGINGS DIENST

# Contactloze Tokens

VNG Realisatie

**Voordelen contactloze tokens:**

- Contactloos apparaat
- Wachtwoorden worden gegenereerd in het device zelf
- Geen netwerk verbinding nodig
- Gaan 5 jaar mee

**Nadelen contactloze token:**

- Verlies of beschadiging kost een nieuw token
- Tokens zijn voor 1 applicatie / toepassing / organisatie (volle sleutelbos))
- Er zijn partijen in de distributieketen die de geheimen kunnen kennen

INFORMATIE BEVEILIGINGS DIENST

# Connected Tokens

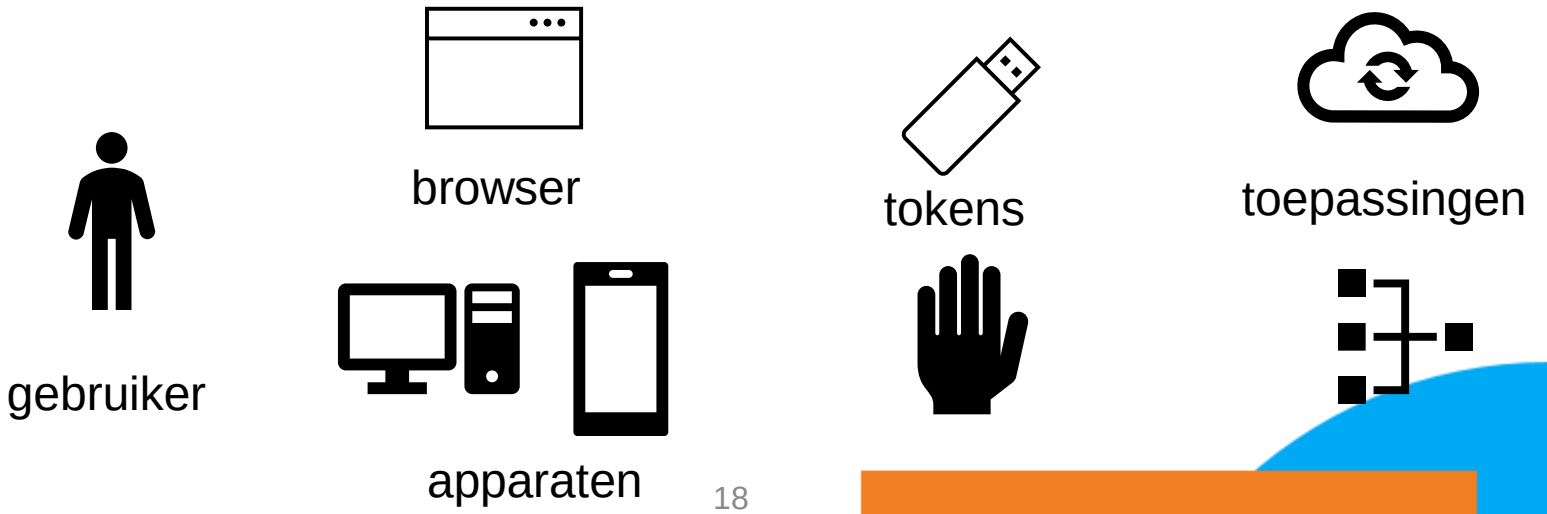
VNG Realisatie

**Voordelen connected tokens**

- Geen verbinding met Internet nodig
- Eén token voor meerdere toepassingen geschikt
- Gebruiksgemak, aansluiten en genereren met een knopdruk / vingerafdruk etc
- Tokens met meerdere soorten aansluitingen bestaan
- Niet kapot te krijgen

**Nadelen connected tokens**

- Jonge techniek, nog niet overal op Internet beschikbaar, hoe integreer je het zelf?
- Niet alle browsers ondersteunen
- Connected: USB poort nodig
- Klein, makkelijk te verliezen
- Kosten



INFORMATIE BEVEILIGINGS DIENST

# Soorten: Apps

VNG Realisatie

- Apps zijn eigenlijk een vervolg op de al oudere SMS standaard
- De meeste apps generen op basis van tijd een 2e factor
- Er zijn wachtwoordkluizen die ook deze functionaliteit hebben
- Voorbeelden: Google authenticator, MS authenticator, Free-OTP

Voordelen:
- Geen mobiele dekking nodig
- Meerdere tokens per app
- Veel keuze

Nadelen:
- Noodzaak om smartphone te gebruiken
- Applicaties kunnen worden gehackt
- Lege batterij = geen code
- Wisselen van telefoon – back-up of migratie kan, of alles opnieuw instellen
- Weerstand bij BYOD

INFORMATIE BEVEILIGINGS DIENST

# SMS

VNG Realisatie

- Werkt op basis van ontvangen van 2e factor d.m.v. SMS
- Wordt soms nog gebruikt
- Laagdrempelig
- Onveilig

Voordelen:
- Eenvoud
- Detectie: Als een sms ontvangen wordt terwijl niks is aangevraagd

Nadelen:
- SMS is niet gratis voor verzender
- Mobiele telefoon nodig
- Netwerk dekking nodig
- Aanvallers kunnen SIM-kaart namaken
- SMS kan worden onderschept

INFORMATIE BEVEILIGINGS DIENST

# 2FA zwakheden?

VNG Realisatie

## Is 2FA dan onfeilbaar?

Zeker niet, er zijn ook aanvallen op 2FA bekend, dit zijn:

- Social engineering aanvallen
- Technische aanvallen
- Een mix van de bovenstaande

Samenvattend:

- 2FA voorkomt geen Phishing of social engineering
- 2FA is noodzakelijk, het is belangrijk de kwetsbaarheden te kennen
- Besteed ook aandacht aan het feit dat 2FA niet onfeilbaar is in bewustwording

Een handig document over 2FA aanvallen kun je hier vinden: https://www.knowbe4.com/hubfs/12+_Ways_to_Hack_Two-Factor_Authentication-1.pdf

INFORMATIE BEVEILIGINGS DIENST

# Vragen

VNG Realisatie

- Zijn er vragen tot zover?

INFORMATIE BEVEILIGINGS DIENST

# Hoe verder: Stappenplan voor de gemeente

VNG Realisatie

1. Stel een Business Case op,
    1. Kosten
    2. Opbrengsten
2. Stel een projectplan op
    1. Scope: waar 2FA inzetten
    2. Op te leveren producten: beleid, architectuur, PVE, Ingevoerde 2FA
3. Voer het project uit
    1. Maak beleid (volgende sheet)
    2. Implementeer de oplossing
    3. Maak beheer mogelijk
    4. Communiceer!
4. In beheer nemen

INFORMATIE BEVEILIGINGS DIENST

# 2FA beleid of ?

VNG Realisatie

- Voeg 2FA toe aan het algemene beveiligingsbeleid van de gemeente, het logisch toegangsbeheer beleid, wachtwoordbeleid en eventueel wachtwoordkluizen beleid.
- Of maak een apart aanvullend 2FA beleid document en bijbehorende procedures

- Beschrijf:
  - waarom 2FA zal worden ingezet
  - waarvoor 2FA zal worden ingezet
  - wanneer 2FA wordt ingezet in welke situaties, welke processen en welke systemen
  - de keuze, welke 2FA de voorkeur heeft binnen de gemeente
  - Hoe

INFORMATIE BEVEILIGINGS DIENST

# Ervaringen gemeenten

VNG Realisatie

- Wie van jullie gebruikt er al 2FA, en waarvoor?
- Wat zijn ervaringen de gemeenten en van de gebruikers?
  - Voor- en nadelen
  - Wat zijn knelpunten
- Wat kost het beheer?
  - Menskracht en financieel
  - Gestegen, gelijk of gedaald?
- Wordt 2FA alleen voor de BIO situatie ingezet of wordt dit breder gebruikt?
  - Intern-intern verkeer en systemen, van binnen naar buiten ipv van buiten naar binnen en beheerders accounts?

INFORMATIE BEVEILIGINGS DIENST

# Vragen

VNG Realisatie

INFORMATIE BEVEILIGINGS DIENST

# Samenvattend

VNG Realisatie

1. Wachtwoorden alleen zijn niet veilig genoeg

2. Zet 2FA niet alleen in voor de BIO eis

3. Zet 2FA in op zoveel mogelijk plaatsen