Deepfakes als bedrijfsrisico

ISACA: ‘The Great Risk Reset’
16 November 2022

Ellen Mok

Senior Consultant, Cyber Strategy and Risk

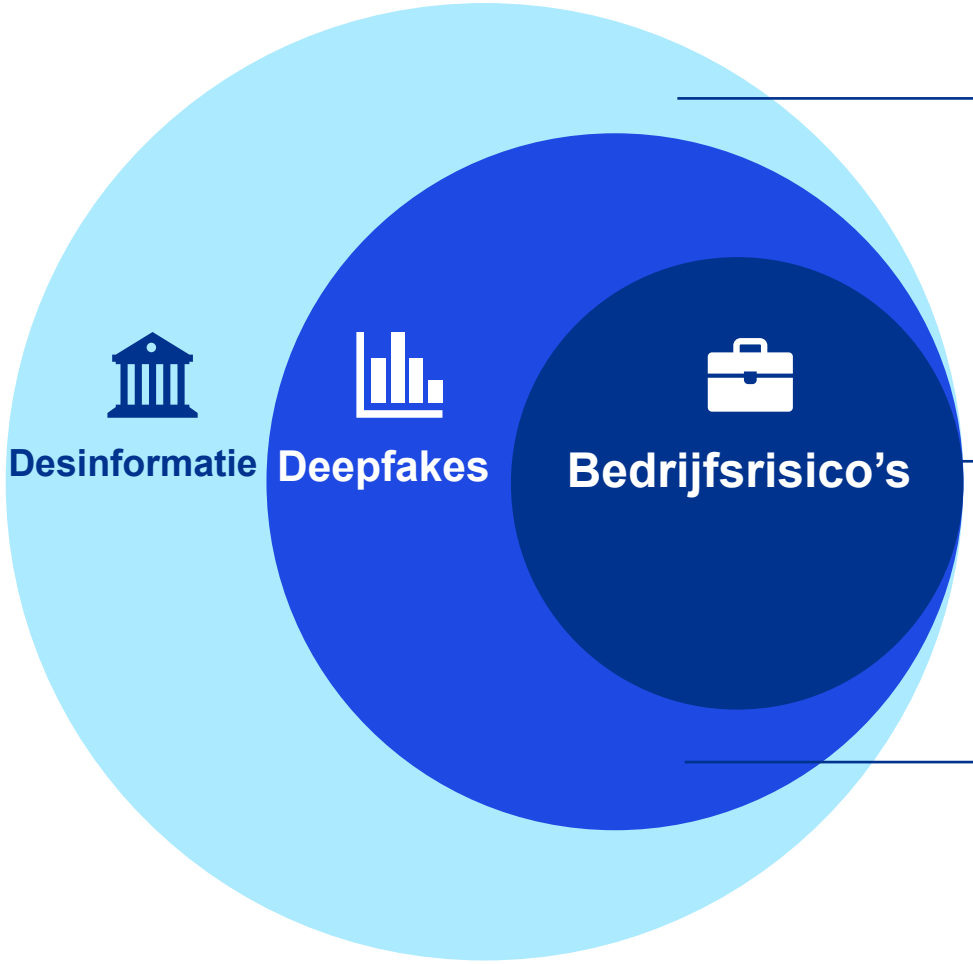
Ervaring:

- Onderzoek en advies over statelijke cyberdreiging
- Digitale weerbaarheid in de publieke sector
- IT-transformatie projecten
- Cyber maturity assessments (CMA)
- Innovatieteam KPMG Cyber S&R

Educatie

- MSc. Engineering and Policy Analysis (TU Delft)
- MSc. Crisis & Security Management (Leiden University)
- BSc. Technische Bestuurskunde (TU Delft)

Deepfakes en desinformatie



Desinformatie

Desinformatie is het opzettelijk verspreiden van onjuiste informatie met het specifieke doel om schade te veroorzaken.

Bedrijfsrisico

Binnen een bredere trend van desinformatie en deepfakes zien wij verschillende bedrijfsrisico's.

Deepfakes

Een deepfake is een vorm van Kunstmatige Intelligentie (A.I.) die gebruikt kan worden om hyper realistische beelden, documenten, en geluiden te creëren.

Desinformatie

Advanced disinformation campaigns will be the second largest cyber threat in 2030

ENISA - top 10 emerging cyberthreats

Desinformatie is opzettelijk onjuiste informatie met het specifieke doel om schade te veroorzaken.

Desinformatie is een middel om doelstellingen te behalen:

- Politieke invloed
- Financieel gewin
- Reputatieschade
- Identiteitsfraude
- ….

Twee interessante mechanismes:

- De reputatie van een bedrijf/industrie, maakt uit hoe mensen desinformatie beoordelen en onthouden.
- Mensen schatten hun eigen vermogen om desinformatie te herkennen vaak hoger in dan dat ze anderen inschatten.

Deepfakes

Deepfakes, synthetic media, and disinformation in general pose challenges to our society

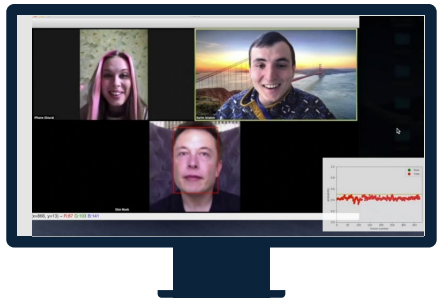
U.S. Homeland Security - Increasing threat of deepfake identities

Een deepfake is een vorm van Kunstmatige Intelligentie (A.I.) die gebruikt kan worden om hyper realistische beelden, documenten, en geluiden te creëren.

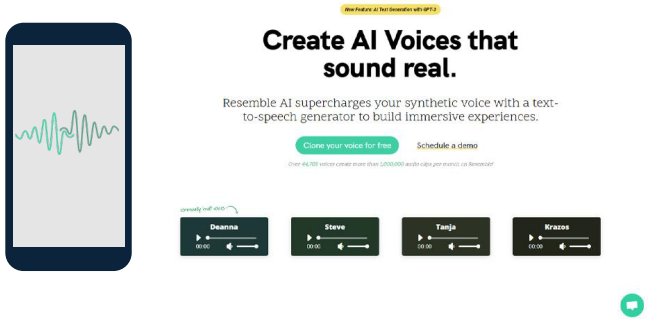
Ook voor deepfakes geldt dat het bekende trends versterkt:

- Politieke invloed
- Pesten
- Vermaak
- Identiteitsfraude
- ….

En dus ook cyberaanvallen:



(Live) video's en foto's



Audio / stemmen (vishing)

Deepfakes

Meldingen van aanvallen met gezichts- en stemveranderende technologie zijn vorig jaar met 13% gestegen

CNET – Deepfakes Pose a Growing Danger

Deepfakes worden al gebruikt bij cyberaanvallen

Stem:

- 2019: “Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case” (source)
- 2020: “Fraudsters Cloned Company Director’s Voice In $35 Million Bank Heist, Police Find” (source)

Video:

- 2021: “Dutch MPs in video conference with deep fake imitation of Navalny's Chief of Staff” (source)

Risico's van deepfake cyberaanvallen

Social engineering

- CEO fraude
- Phishing
- Voordoen als financiële institutie

Manipulatie aandelen

- Aankondiging verkoop van aandelen of producten

Identiteitsfraude

- Toegang tot persoonlijke omgevingen
- Valse klantprofielen
- Voordoen als een bekende om geld over te maken

Beschadigen reputatie

Toegeven van:

- Criminele activiteiten
- (nieuwe) Activiteiten van de organisatie
- Investeringen.

Pesten

- Op de werkvloer
- Fake porno van (mogelijke) werknemer

Geavanceerde aanvallen

- Verkrijgen van toegang tot privé netwerk via familieleden
- Vals bewijs in een rechtszaak
- Valse kidnappings voor losgeld

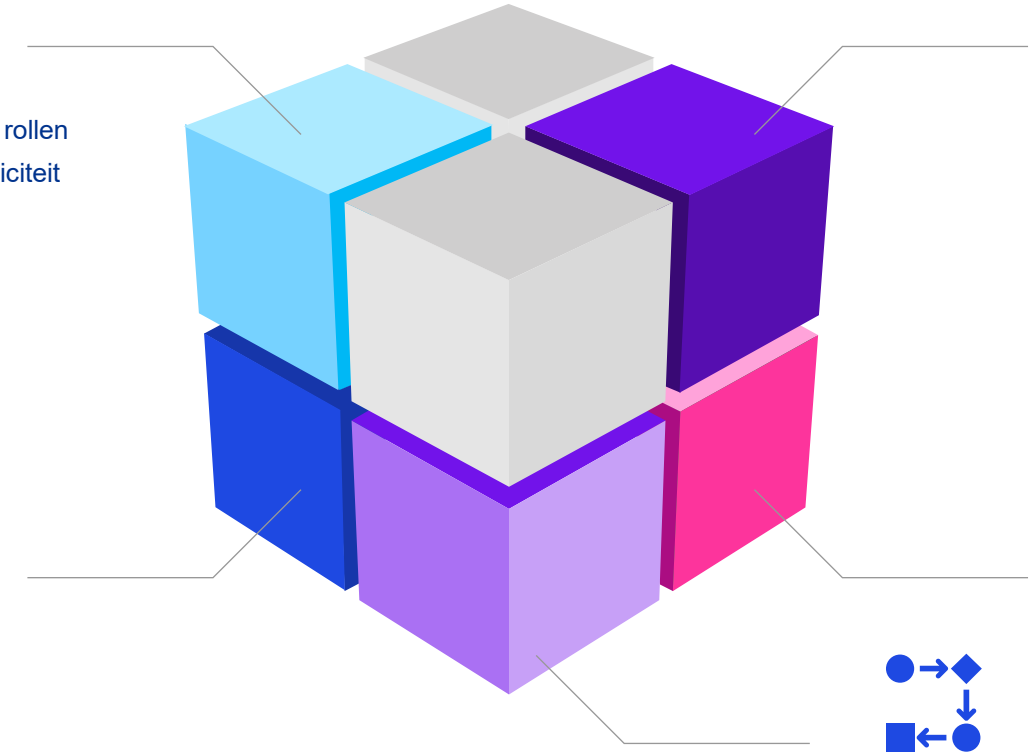
Bescherm jezelf tegen deepfakes

Awareness

- Training
- Speciale training voor bepaalde rollen
- Focus op verificatie van authenticiteit zender

Authenticatie methoden

- Blockchain
- MFA
- Certificaten



Detectie

- CTI
- Deepfake detectie programma's

"Response strategy"

- Communicatie
- Forensisch onderzoek
- Test response strategieën!

Procedures

- Bestaande procedures
- Nieuwe procedures

Contact

Wij nodigen je graag uit om met ons te sparren over de risico's van deepfakes voor jou organisatie

Ellen Mok - KPMG

Ellen Mok

M: +31 6 42718256

E: mok.ellen@kpmg.nl

L: Ellen Mok | LinkedIn

Jim Boevink

M: +31 6 51379548

E: boevink.jim@kpmg.nl

L: Jim Boevink | LinkedIn

Marijn Pronk

M: +31 6 23010796

E: pronk.marijn@kpmg.nl

L: Marijn Pronk | LinkedIn

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

Document Classification: KPMG Public