mbo digitaal

NETWERK
Informatiebeveiliging
en Privacy

Nulmetingen cyberveiligheid

als start van het programma Cyberveiligheid mbo

1. Volwassenheidsmeting Informatiebeveiliging
   > resultaten & conclusies
2. Governance
3. Awarenessmeting
4. Crisismanagement
5. Technische weerbaarheid
6. Red Teaming

Martijn Bijleveld
MBO Digitaal
m.bijleveld@mbodigitaal.nl

Programma Cyberveiligheid mbo

- Gecoördineerd door MBO Raad / MBO Digitaal
- Afstemming met:
  - netwerk IBP (via regiegroep IBP)
  - contactpersonen SURF (via CSC-overleg)
  - Innovatiezone SURF (via regiegroep IZ)
- Uitvoering in principe door- of samen met SURF
  - samenwerkingsovereenkomst
- Samenwerken met FO en HO waar zinvol
- Subsidieaanvraag 24 mln goedgekeurd
- Per 1 oktober 2022 gestart

MBO Raad

mbo digitaal

Cyberveiligheid in het mbo

Plan van aanpak om de digitale weerbaarheid en de privacybescherming van de mbo-instellingen te verhogen

MBO Digitaal & MBO Raad
Versie 1.7
2 september 2022

mbo digitaal

Programma Cyberveiligheid mbo

- Identificeren van dreigingen en risico's (*identify*)
- Beschermen tegen cyberrisico's (*protect*)
- Detecteren van onregelmatigheden (*detect*
- Reageren op incidenten (*respond*)
- Herstellen van incidenten (*recover*)
- Cloudleveranciers

mbo digitaal

Programma start met nulmetingen

1. Volwassenheid Informatiebeveiliging
2. Governance
3. Awarenessmeting
4. Crisismanagement
5. Technische weerbaarheid
6. Red teaming assessments

mbo digitaal

Nulmeting volwassenheid Informatiebeveiliging

Uitgevoerd in oktober 2022, in plaats van Benchmark IBP

Ingevuld door 49 mbo-instellingen:

- **actuele** volwassenheid
- **streefvolwassenheid** op basis van risico-inschatting
- **prognose** volwassenheid in oktober 2023

Op basis van het nieuwe NBA-toetsingskader

mbo digitaal

NBA-volwassenheidsmodel in 21 thema's

Governance		Processen		Technische weerbaarheid	
G01	Strategie	P08	Human Resources	T15	MFA - Thuiswerken
G02	Beleid	P09	ITIL	T16	SOC SIEM
G03	Architectuur	P10	Datamanagement	T17	Pentesten
G04	Eigenaarschap	P11	IAM	T18	Patchbeheer
G05	Risk Management	P12	Security Baselines	T19	Infrastructuur
G06	Roadmap	P13	Business Continuïteit	T20	Security Policy
G07	Toetsing	P14	Cloud Leveranciers	T21	Computer Operations

Bestuur

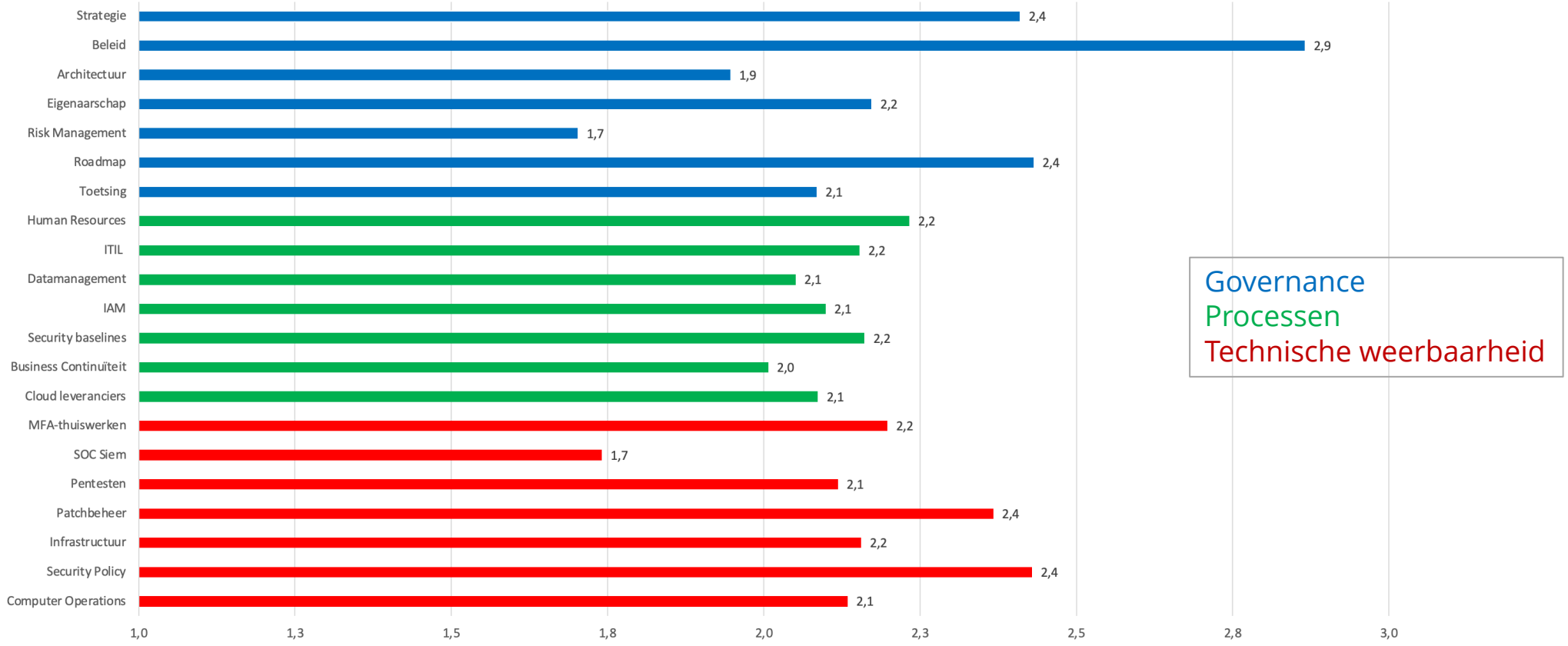
Proceseigenaren

IT

mbo digitaal

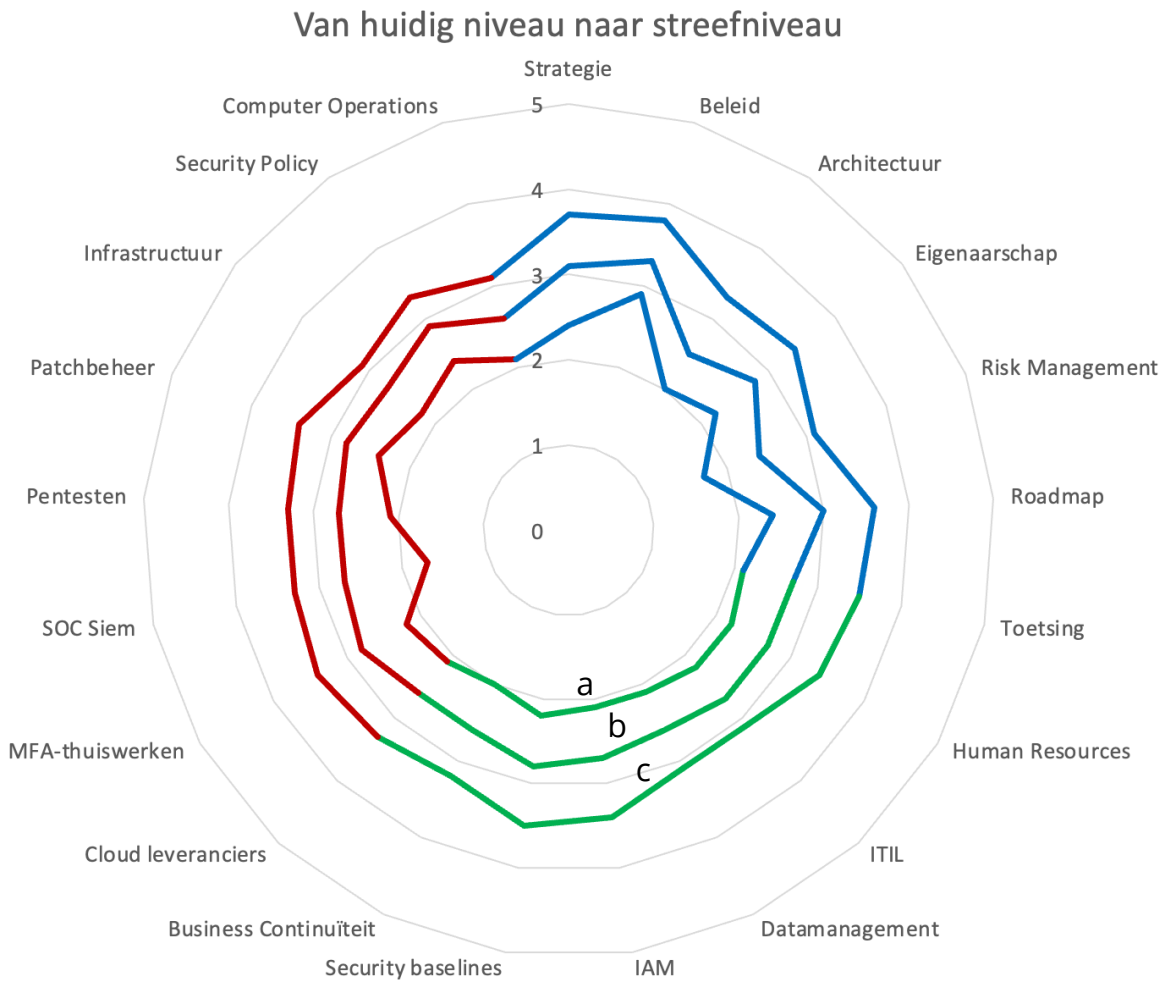
Nulmeting volwassenheid Informatiebeveiliging

Actuele volwassenheid is gemiddeld 2,1 (n=49)



mbo digitaal

Nulmeting volwassenheid Informatiebeveiliging



Groei in volwassenheid

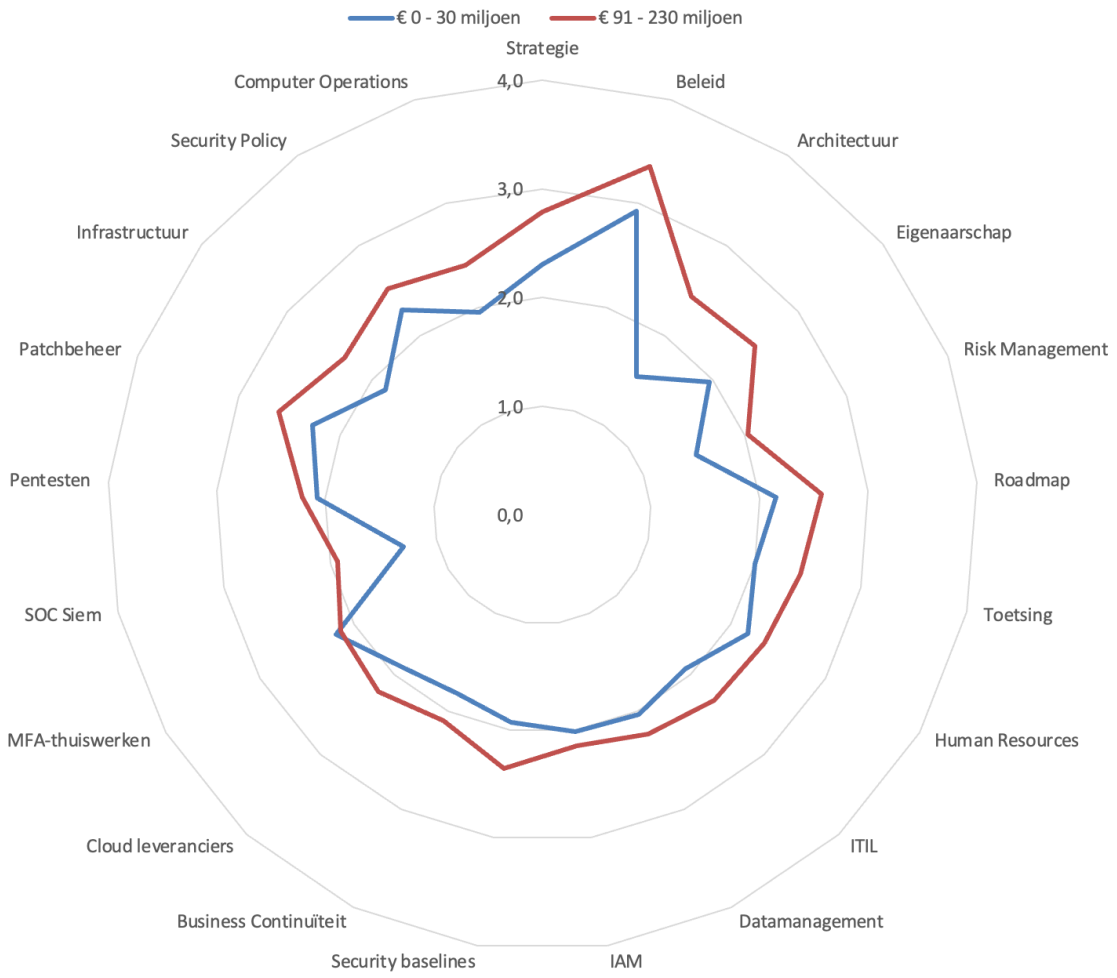
a) Actuele volwassenheid (IST): 2,1
b) Prognose Q3 - 2023: 2,8
c) Streefvolwassenheid (SOLL): 3,3

Governance
Processen
Technische weerbaarheid

- Enorme ambitie!
- Input voor het programma

mbo digitaal

Nulmeting volwassenheid Informatiebeveiliging



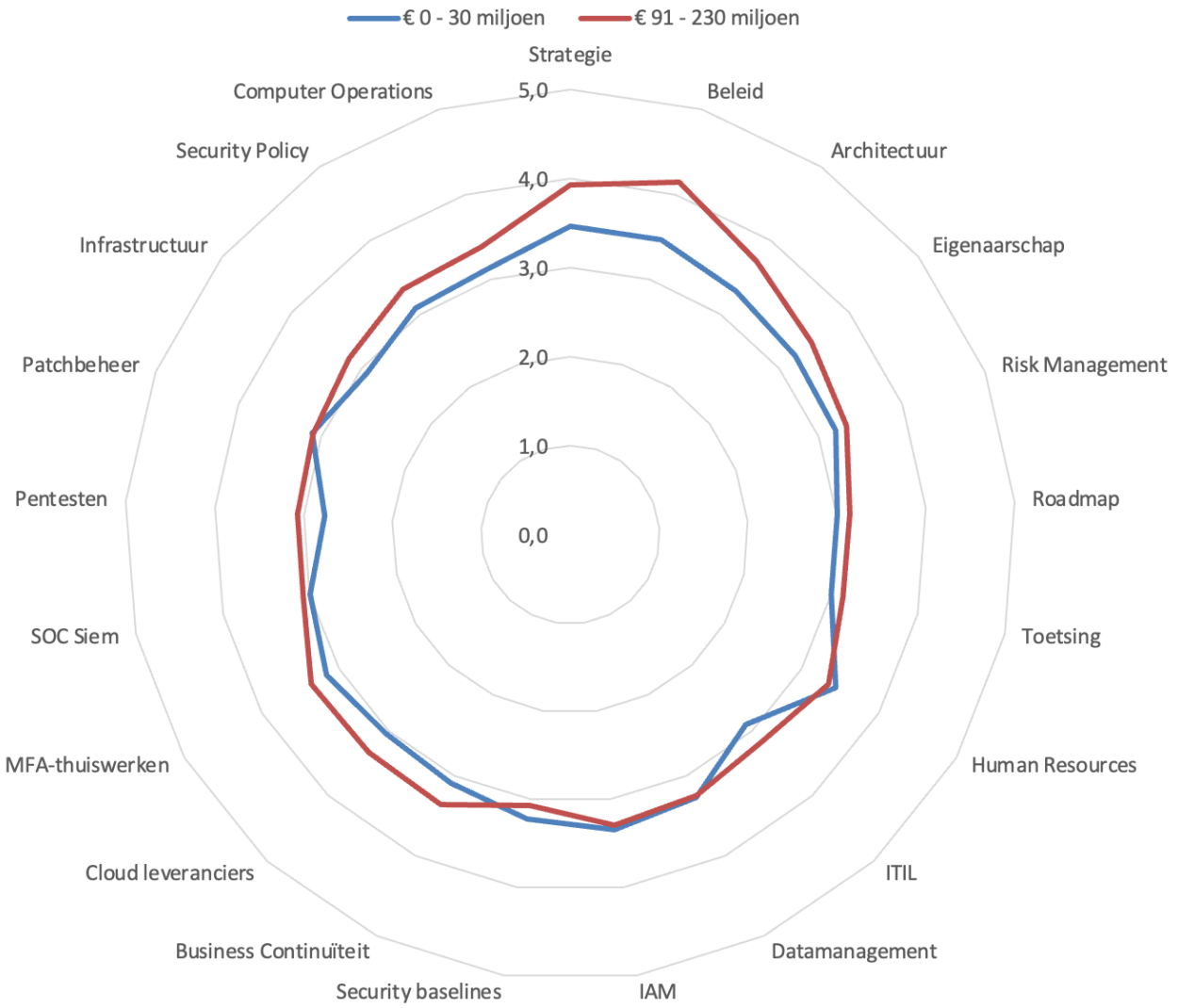
Vergelijking actuele volwassenheid tussen kleine en grote instellingen

Gemiddelde actuele volwassenheid

- kleine instellingen: 2,0
- grote instellingen: 2,3

mbo digitaal

Nulmeting volwassenheid Informatiebeveiliging



Vergelijking streefvolwassenheid tussen kleine en grote instellingen

Gemiddelde streefvolwassenheid

- kleine instellingen: 3,1
- grote instellingen: 3,3

mbo digitaal

Nulmeting governance

Enquete-instrument gericht op IPB-functie en de rol van het bestuur

- Houding en zorg CvB ten aanzien van IBP
- Rol en betrokkenheid van het CvB en het MT
- IBP-beleid, TBV’s & eigenaarschap
- De plaats van de IBP-functionaris in de organisatie
- Totstandkoming budgetten IBP

mbo digitaal

Nulmeting governance

Welke orgaan/functionaris is eindverantwoordelijke voor het opstellen van jaarplannen ten aanzien van informatieveiligheid? *

- CvB
- Management Team (
- Proceseigenaar
- In de lijn / lijnmanag
- Manager F&C
- Manager ICT
- IB Stuurgroep
- IB functionaris

Ambities met betrekking tot informatiebeveiliging zijn geformuleerd en vastgesteld. *

- Volledig me
- Enigszins m
- Niet eens -
- Grotendeels
- Volledig me

Het CvB is betrokken bij het vaststellen van beleid ten aanzien van informatieveiligheid en privacy. *

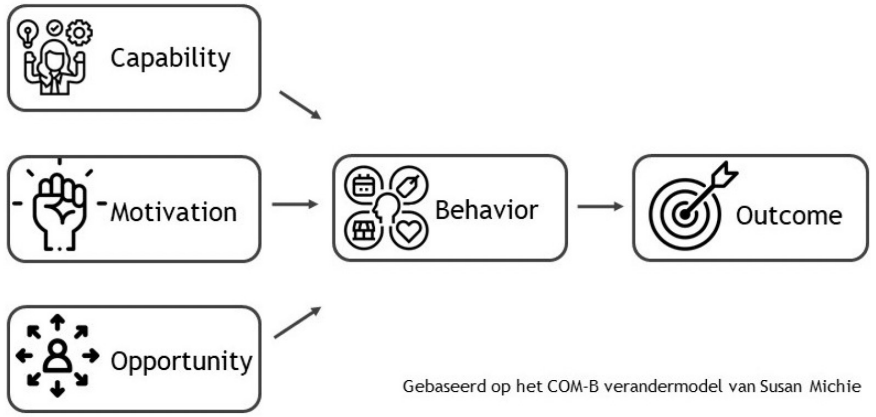
- Volledig mee eens
- Enigszins mee eens
- Niet eens - niet mee on
- Grotendeels mee oneer

Hoe vaak wordt vanuit het CvB de voortgang van bela gecontroleerd? *

- Maandelijks
- Twee maandelijks

mbo digitaal

Awarenessmeting



- Instrument BDO, 2x gebruikt voor Awarenessmeting SURF
  - deelname vanuit mbo zeer beperkt
- Kennisvragen toegesneden op het mbo
- In voorjaar 2023 breed uitgezet binnen het mbo
  - door IBP-contactpersonen, ondersteund met communicatie vanuit MBO Raad / MBO Digitaal
  - afnameperiode 1 april - 22 mei 2023
- Uitkomsten zijn input voor (awareness)activiteiten binnen het programma Cyberveiligheid mbo

mbo digitaal

Nulmeting crisismanagement

Op basis van verwachtingen en ervaringen oefenleiders OZON 2023

- Verantwoordelijkheden, taken & rollen
- Communicatie
- Incident management
- Crisismanagement / bedrijfscontinuïteitsbeheer
- Operationele IT
- Kennis & Kunde
- Gedrag en samenwerking

mbo digitaal

Nulmeting crisismanagement

Thema	Stellingen voor oefenvoorbereider
Verantwoordelijkheden, taken & rollen	Tijdens een crisis zal het duidelijk zijn wie de eigenaren zijn van bepaalde processen, systemen en data, en zij nemen daarin hun verantwoordelijkheid.
	De medewerkers zullen zich bewust zijn van hun formeel toegewezen rol en de daarbij behorende verantwoordelijkheden en taken.
	Beslissingen zullen worden genomen door de juiste persoon, op de juiste tijd en op het juiste organisatieniveau (strategisch, tactisch, operationeel).
	Het personeel zal tijdens een crisissituatie alleen geautoriseerde taken uitvoeren die bij hun respectievelijke functies en rol horen.
Communicatie	Er zijn formele comunicatielijnen in de organisatie en medewerkers kunnen deze gemakkelijk raadplegen indien nodig.
	Er zal een correcte crisislogging plaatsvinden.
	Bij de wisseling van de wacht zullen de werkzaamheden adequaat worden overgedragen, indien van toepassing.
	Andere onderwijsins
	Er zal een landelijke
Incident management	Medewerkers zulle
	Oorzaken van (pote
	Er zijn escalatiepade
Crisismanagement / bedrijfscontinuïteitsbeheer	Er is een duidelijk be
	Het continuïteitsplar
	De organisatie besc
	Er is een actuele (da
Operationele ICT	Er is een actueel ov
	Er is een actueel ov
	Er is een actueel ov
Kennis & Kunde	Medewerkers besc
	Medewerkers besc
	De organisatie zal in
Gedrag en samenwerking	Het management z
	Tijdens een crisis za
	Tijdens een crisis za

Thema	Stellingen voor oefenvoorbereider
Verantwoordelijkheden, taken & rollen	Tijdens de crisis was het duidelijk wie de eigenaren zijn van bepaalde processen, systemen en data, en zij nemen daarin hun verantwoordelijkheid.
	De medewerkers waren zich bewust van hun formeel toegewezen rol en de daarbij behorende verantwoordelijkheden en taken.
	Beslissingen zijn genomen door de juiste persoon, op de juiste tijd en op het juiste organisatiniveau (strategisch, tactisch, operationeel).
	Het personeel voerde tijdens de crisis alleen geautoriseerde taken uit die bij hun respectievelijke functies en rol horen.
Communicatie	Er zijn formele comunicatielijnen in de organisatie en medewerkers hebben deze kunnen raadplegen.
	De communicatielijnen zijn correct geraadpleegd en gebruikt door medewerkers.
	Er heeft een correcte crisislogging plaatsgevonden.
	Andere onderwijsinstellingen waren bereikbaar om samen te werken en kennis te delen en deze communicatie liep voorspoedig.
	Er was een landelijke of sectorbrede coördinatie voor samenwerking en kennisdeling en deze is waardevol geweest.
Incident management	Medewerkers waren in staat om risicovolle situaties en mogelijke incidenten te herkennen en deze adequaat te beoordelen.
	Oorzaken van (potentiële) incidenten en problemen tijdens de crisis zijn beheerst totdat ze worden opgelost.
	Er zijn escalatiepaden geformaliseerd in de organisatie, en medewerkers hebben hier gebruik van gemaakt tijdens het afhandelen van incidenten.
Crisismanagement / bedrijfscontinuïteitsbeheer	Er is een duidelijk bedrijfscontinuïteitsplan/crisisplan geformaliseerd in de organisatie en medewerkers hebben dit kunnen raadplegen.
	Het continuïteitsplan is correct gebruikt als leidraad voor de crisis door medewerkers.
	Er is op het correcte moment opgeschaald.
	Het crisisplan is correct geraadpleegd en gebruikt door medewerkers.
	Het is duidelijk welke bedreigingen en kwetsbaarheden van toepassing zijn op de organisatie en hier is adequaat mee omgegaan tijdens de crisis.
	Er is een actuele (data) classificatie te raadplegen om tijdens een crisis processen juist te kunnen prioriteren en medewerkers wisten dit te vinden..
Operationele ICT	Er is een actueel overzicht met alles dat is aangesloten aan het netwerk met welke functie het heeft en wie de eigenaar is, en medewerkers wisten dit te vinden.
	Er is een actueel overzicht met software waar de organisatie gebruik van maakt en wie de eigenaar is, en medewerkers wisten dit te vinden.
	Er is een actueel overzicht van de netwerkarchitectuur dat geraadgpleegd kan worden, en medewerkers wisten dit te vinden.
	Medewerkers beschikken vanuit hun rol over voldoende kennis om problemen te analyseren.

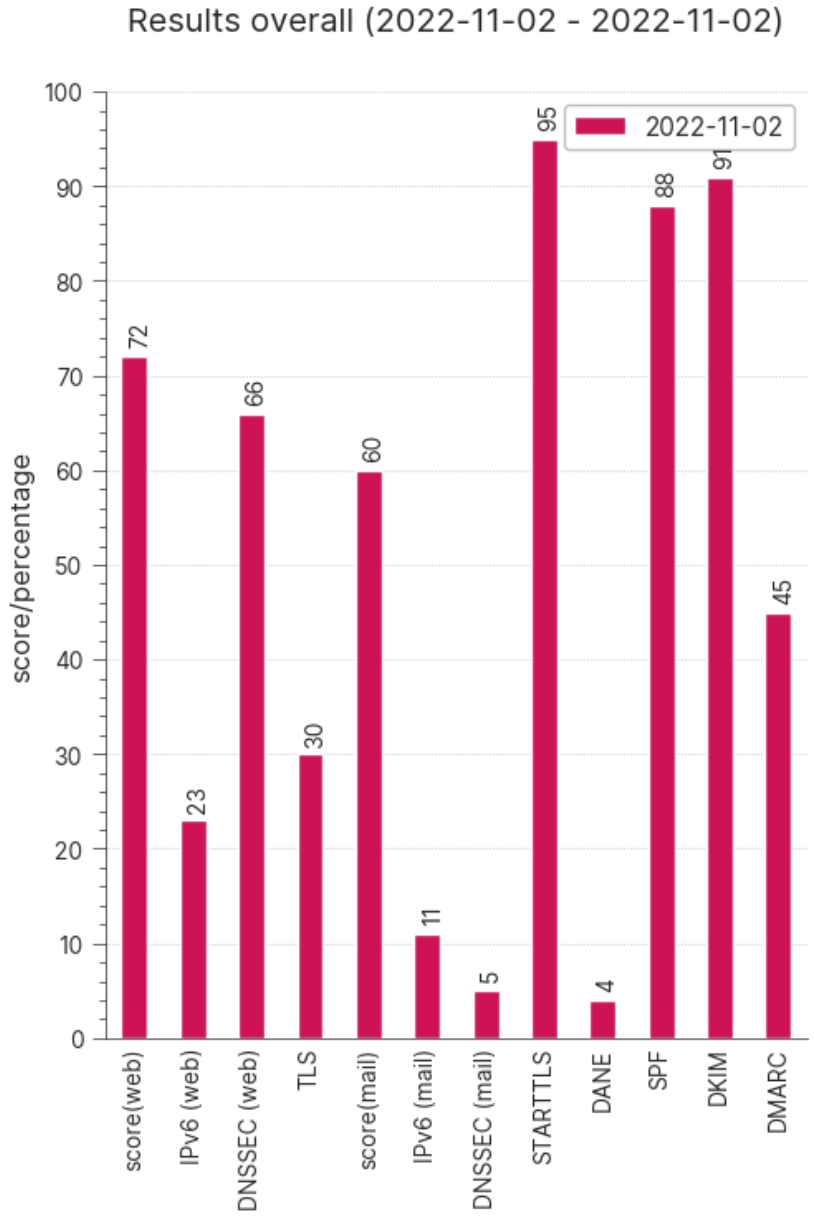
mbo digitaal

Nulmeting technische weerbaarheid

Laaghangend fruit: IV-metingen

- meting uitgevoerd voor alle mbo-instellingen (ook niet-leden)
- behoefte aan duiding: waarom belangrijk
- behoefte aan instructie: ze doe je het (in MS365)
- wordt uitgewerkt binnen SEC

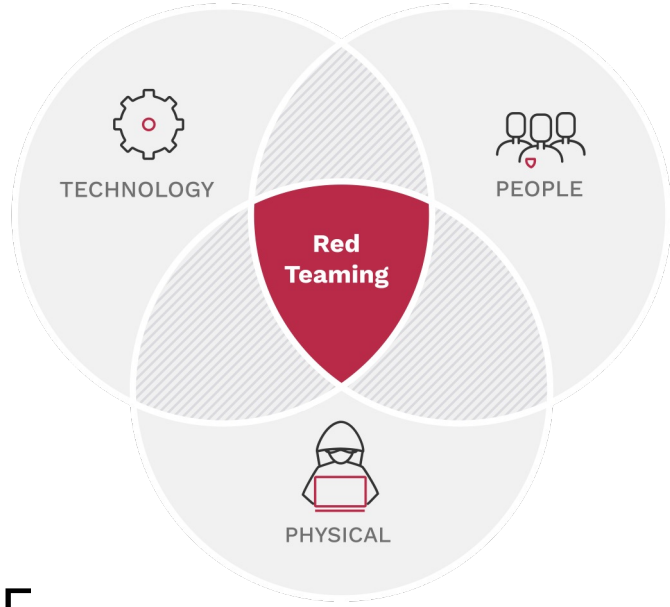
Andere vormen (zoals vulnerability scanning en pentesting) worden onderzocht.



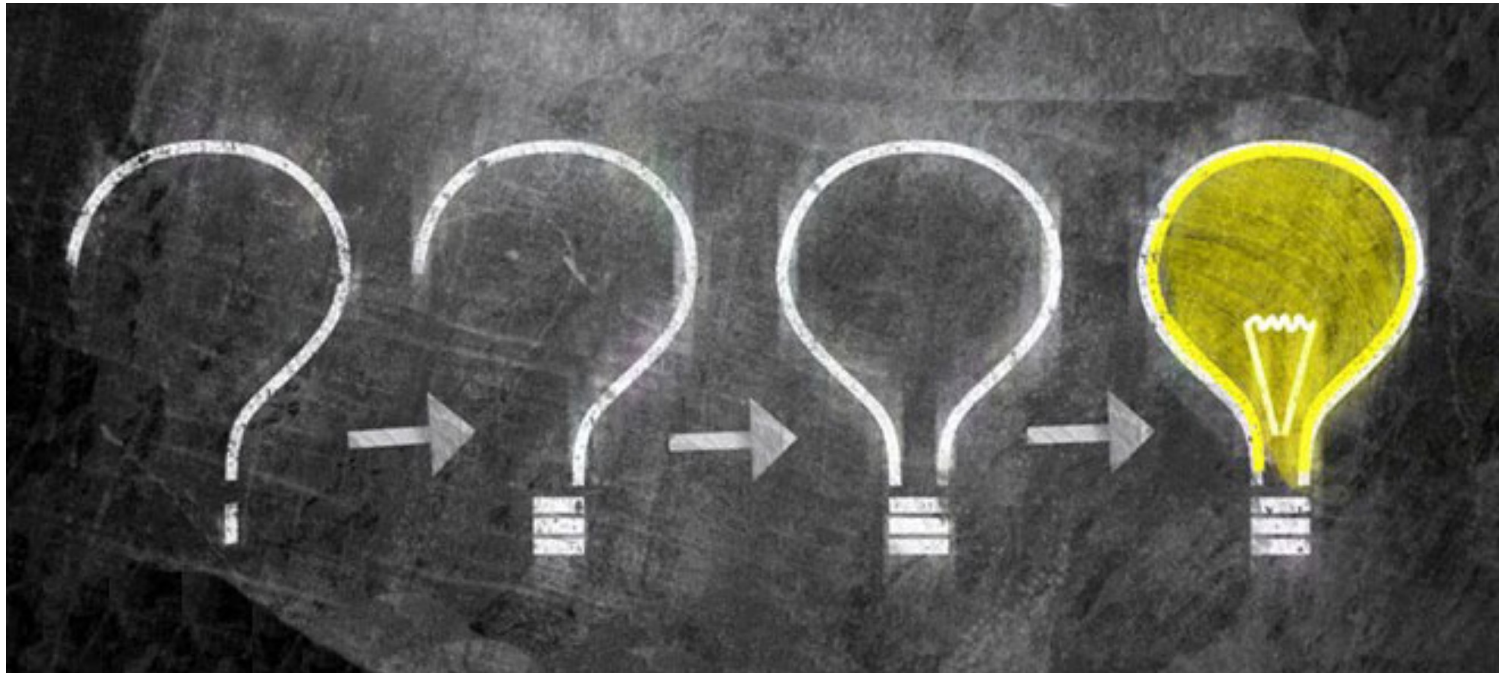
mbo digitaal

Afsluiten met een red teaming oefening

Afsluitende red teaming oefening
  - menselijke factor
  - fysieke beveiliging
  - technische weerbaarheid
- Voor 3 mbo-instellingen
- Light-aanpak (€100K)
- Binnen raamwerk voor weerbaarheidstesten SURF
  - SURF vormt het white team
- Selectie mbo's op basis van resultaten nulmetingen en intake
- Delen van de opbrengsten via netwerk IBP en SEC



Vragen en discussie



Martijn Bijleveld
MBO Digitaal
m.bijleveld@mbodigitaal.nl