mbo digitaal

NETWERK
Informatiebeveiliging
en Privacy

Programma Cyberveiligheid mbo

De hoofdlijnen van het programma Cyberveiligheid

Gebruikersdag MBO Digitaal, 6 februari 2023

Martijn Bijleveld

Adviseur IBP

Programmamanager
Cyberveiligheid mbo

MBO Digitaal

mbo digitaal

Onderwijs onder vuur

HvA en UvA getroffen door cyberaanval

De Hogeschool van Amsterdam (HvA) en Universiteit van Amsterdam (UvA) zijn doelwit van een cyberaanval. Onbekenden 'hebben zich toegang verschaft tot de ICT-omgevingen van de HvA en UvA', schrijft de universiteit.

Het Parool 17 februari 2021, 13:16

BEELD ANP

De universiteit onderzoekt nog welke delen van de ICT-omgeving zijn geraakt.

Om de gevolgen te beperken en ervoor te zorgen dat onderwijs en onderzoek door kunnen gaan, worden komende tijd systemen tijdelijk uitgezet. Dat betekent dat die systemen, en de informatie in die systemen, niet beschikbaar zijn op dat moment.

deVolkskrant

Hogeschool InHolland gehackt: persoonlijke gegevens tienduizenden studenten aangeboden op internetforum

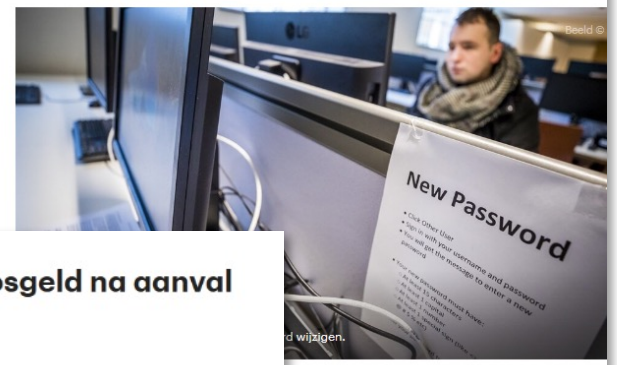
Hackers bieden op een internetforum persoonlijke gegevens van 56.000 studenten van InHolland aan. I zijn vorige maand buitgemaakt. De hack past in een groeiende trend waarbij organisaties met veel persoonsgegeve

Laurens Verhagen 1 m

Grote cyberaanval

Universiteit Maastricht betaalde 197.000 euro losgeld aan hackers

05 februari 2020 15:12
Aangepast: 05 februari 2020 20:38



Beeld ©

d wijzigen.

eft bijna twee ton aan losgeld betaald
rsitaire computersystemen kort voor
l platlegden.

Ransomware

Staring College betaalt losgeld na aanval met gijzelsoftware

26 februari 2021 20:59

ring College in de Gelderse p
betaald aan hackers die de s

▲ Nijmeegse studenten van de HAN. © David van Haren

HAN: 4300 wachtwoorden gelekt, totale omvang hack nog niet bekend

ARNHEM/NIJMEGEN De Hogeschool Arnhem & Nijmegen heeft 4300 mensen een mail gestuurd dat hun wachtwoord is gelekt nadat een hacker inbrak in systemen van de hogeschool. Het gaat om oudere wachtwoorden die voor 2018 zijn gebruikt om in te loggen op systemen

26 vestigingen

Grote hack bij ROC Mondriaan: computers plat en bestanden ontoegankelijk

23 augustus 2021 16:29

Beeld © ANP

Studenten van het ROC Mondriaan in 2021.

Onderwijsinstelling ROC Mondriaan in Den Haag is afgelopen weekend gehackt door criminelen. De computers liggen plat en

mbo digitaal

Onderwijs onder vuur

HvA en UvA getroffen door cyberaanval

De Hogeschool van Amsterdam (HvA) en Universiteit van Amsterdam (UvA) zijn doelwit van een cyberaanval. Onbekenden 'hebben zich toegang verschaft tot de ICT-omgevingen van de HvA en UvA', schrijft de universiteit.

Het Parool 17 februari 2021, 13:16

BEELD ANP

De universiteit onderzoekt nog welke delen van de ICT-omgeving zijn geraakt.

Om de gevolgen te beperken en ervoor te zorgen dat onderwijs en onderzoek door kunnen gaan, worden komende tijd systemen tijdelijk uitgezet. Dat betekent dat die systemen, en de informatie in die systemen, niet beschikbaar zijn op dat moment.

Hogeschool … gehackt: per… gegevens tie… studenten a… internetfor…

Hackers bieden op e… gegevens van 56.000… zijn vorige maand b… groeiende trend wa… persoonsgegeven…

Laurens Verhagen 1 ma…

fd. Mijn nieuws Net binnen Beurs Krant Podcasts

Reconstructie • 11 jan 06:00

Cyberaanval op het Nova College: 'Elke minuut extra geeft de hackers meer mogelijkheden'

Stijn van Gils

Net voor kerst ontdekte het Haarlemse Nova College verdachte activiteiten op zijn netwerk. Om hackers de pas af te snijden, besloot de onderwijsinstelling met 13.000 studenten al zijn systemen af te sluiten van de buitenwereld. Een reconstructie van een reddingsoperatie.

Grote cyberaanval

Universiteit Maastricht betaalde 197.000 euro losgeld aan hackers

05 februari 2020 15:12
Aangepast: 05 februari 2020 20:38

…bijna twee ton aan losgeld betaald …ire computersystemen kort voor …atlegden.

… Mondriaan: computers …ontoegankelijk

Beeld © ANP

… ROC Mondriaan in Den Haag is afgelopen …door criminelen. De computers liggen plat en

mbo digitaal

Cyber-wedloop

- Universiteit Maastricht €200.000 > ROC Mondriaan €4.000.000
- Professionalisering van disciplines
  - Phishing aanvallen
  - Inbraak netwerk, bemachtigen rechten
  - Exfiltratie data
  - Ransomware onwikkelen (RaaS)
  - Ransomware uitrollen en afhandelen
  - Verkoop gestolen gegevens

Happy Blog

Blog search Search

KASEYA ATTACK INFO

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70 000 000$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.

mbo digitaal

Op de politieke agenda

Ikzelf heb zeer recent met de verschillende koepels gesproken over de verhoging van de weerbaarheid tegen cyberdreigingen. Bij alle partijen bestaat een gedeeld gevoel van urgentie om extra maatregelen te treffen en grote overeenstemming over de richting en het doel dat we willen bereiken. Vanzelfsprekend is soms differentiatie nodig – instellingen zijn niet gelijk qua grootte en risicoprofiel – maar deze differentiatie doet niets af aan de gedeelde urgentie en het gedeelde eindbeeld.
Hieronder ga ik nader in op de te nemen maatregelen. Kernelementen zijn dat elke instelling in het MBO en HO aan een vooraf afgesproken streefdoel voldoet, dat elke instelling wordt aangesloten op een mechanisme om 24/7 dreigingen te monitoren en dat elke instelling zich periodiek (ook) extern laat auditen. Zoals gezegd is maatwerk daarbij noodzakelijk. In het eerste kwartaal van 2022 wil ik met de sectoren een plan van aanpak met een kalender wanneer dit voor elke instelling gerealiseerd kan zijn. Verder draag ik zorg voor voldoende informatie (loketfunctie) vanuit het NCSC en de veiligheidsdiensten over dreigingen,

Kamervragen 21 sep 2021

Antwoord op vragen van de leden Van Meenen en Van Ginneken over het bericht dat het ROC Mondriaan in Den Haag is gehackt 2021D34616

dat het ROC **Mondriaan** in Den Haag is gehackt (ingezonden 30 augustus 2021). Antwoord van Minister Van Engelshoven (Onderwijs, Cultuur en Wetenschap) (ontvangen 21 september 2021). Vraag 1 Bent u bekend met het artikel...

Brieven regering 28 sep 2021

Digitale weerbaarheid in het hoger onderwijs en onderzoek en in het middelbaar beroepsonderwijs 2021D35537

Digitale weerbaarheid in het hoger onderwijs en onderzoek en in het middelbaar beroepsonderwijs. -. Middelbaar beroepsonderwijs Zoals eerder in deze brief beschreven, gelden veel van de maatregelen zowel voor het hoger als...

Kamervragen 20 sep 2021

Antwoord op vragen van de leden El Yassini en Rajkowski over het bericht 'Grote hack bij ROC Mondriaan: computers plat en bestanden ontoegankelijk' 2021D

gaat zoals klassenlijsten, mails en financiële gegevens van ROC **Mondriaan**. ROC **Mondriaan** zal de studenten, cursisten en medewerkers die het betreft zo snel mogelijk hierover informeren. Vraag 6 Is er contact geweest tussen het...

mbo digitaal

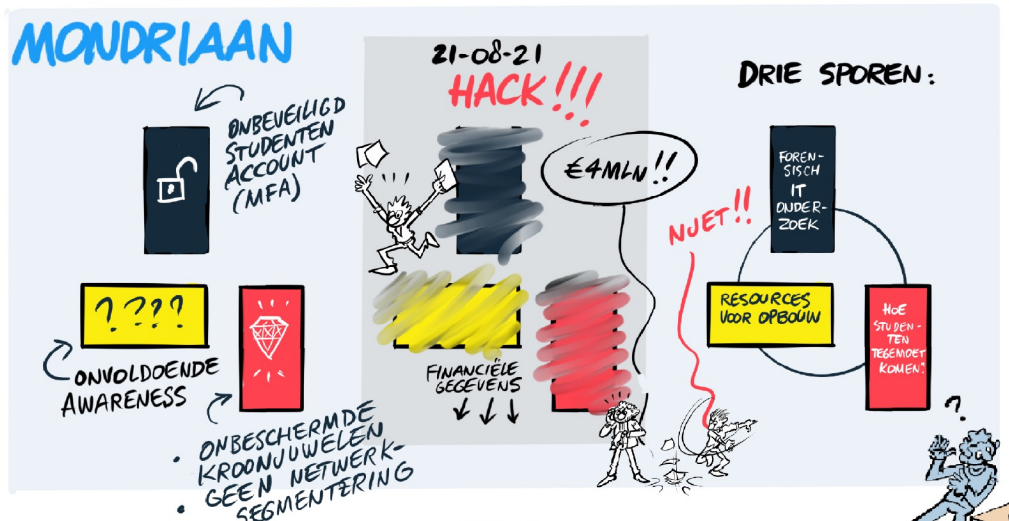
WELKOM 123

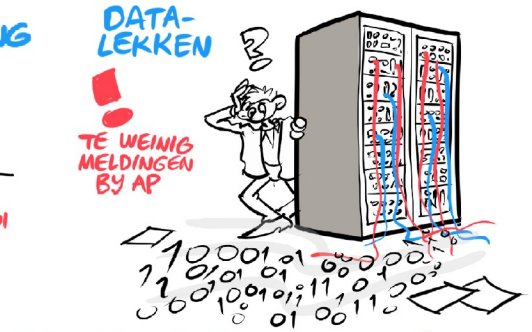
MBO-RAAD 6 DECEMBER 2021 + MINISTERIE OC&W, INSPECTIE VAN HET ONDERWIJS, AUTORITEIT PERSOONSGEGEVENS

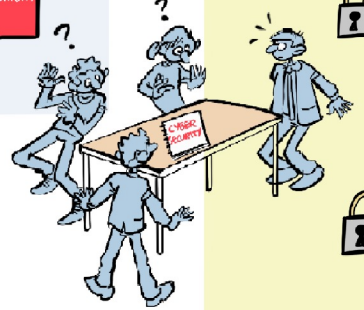
BESTUURDERSBIJEENKOMST CYBERSECURITY

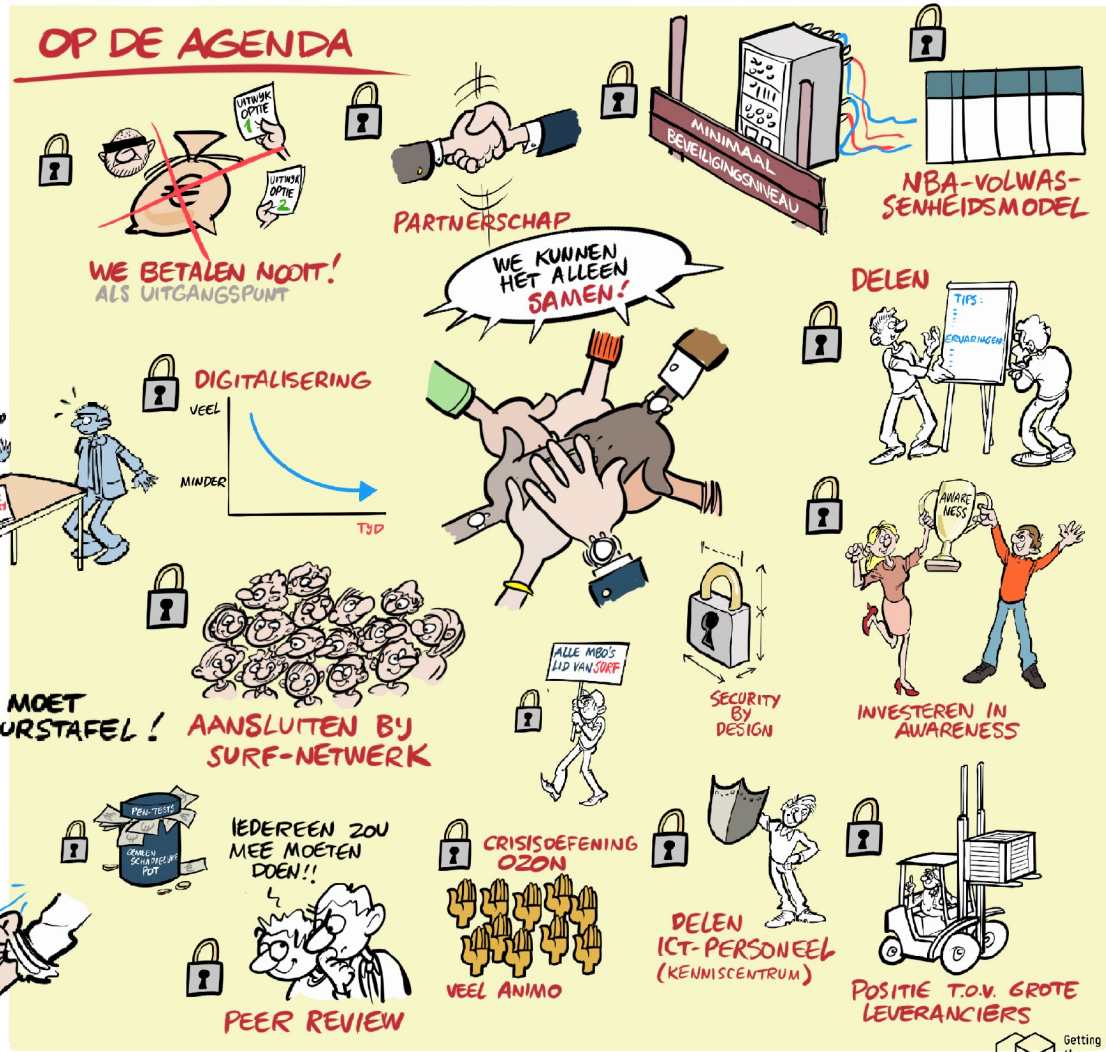
ZEER GEÏNTERESSEERD VAN WIE 38 BESTUURDER

- 69 DEELNEMERS
- 39 MBO-INSTELLINGEN



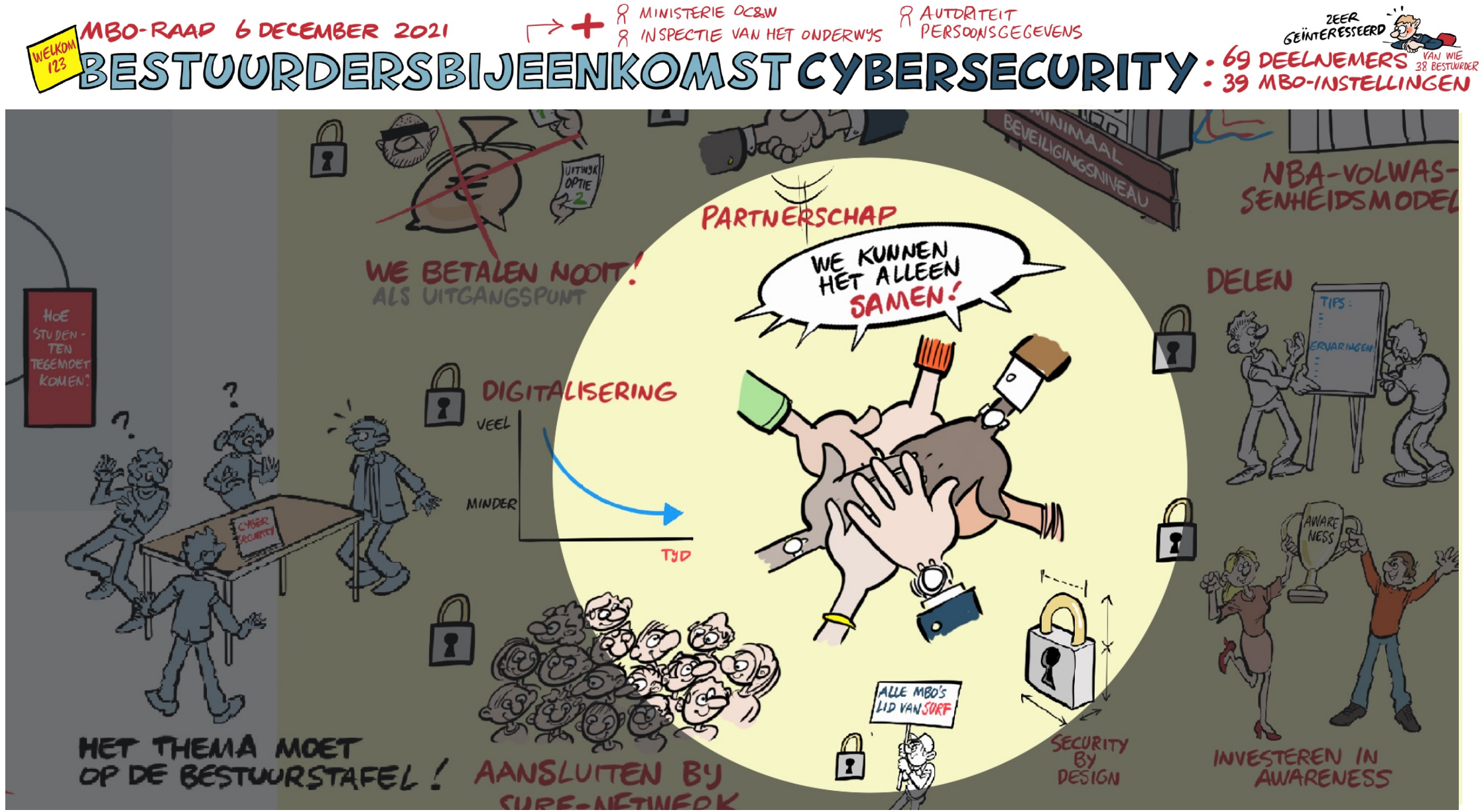






Getting the picture.

mbo digitaal



mbo digitaal

Programma Cyberveiligheid mbo

- Gecoördineerd door MBO Raad / MBO Digitaal
- Afstemming met Netwerk IBP & CSC's
- Uitvoering in principe door- of samen met SURF
- 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

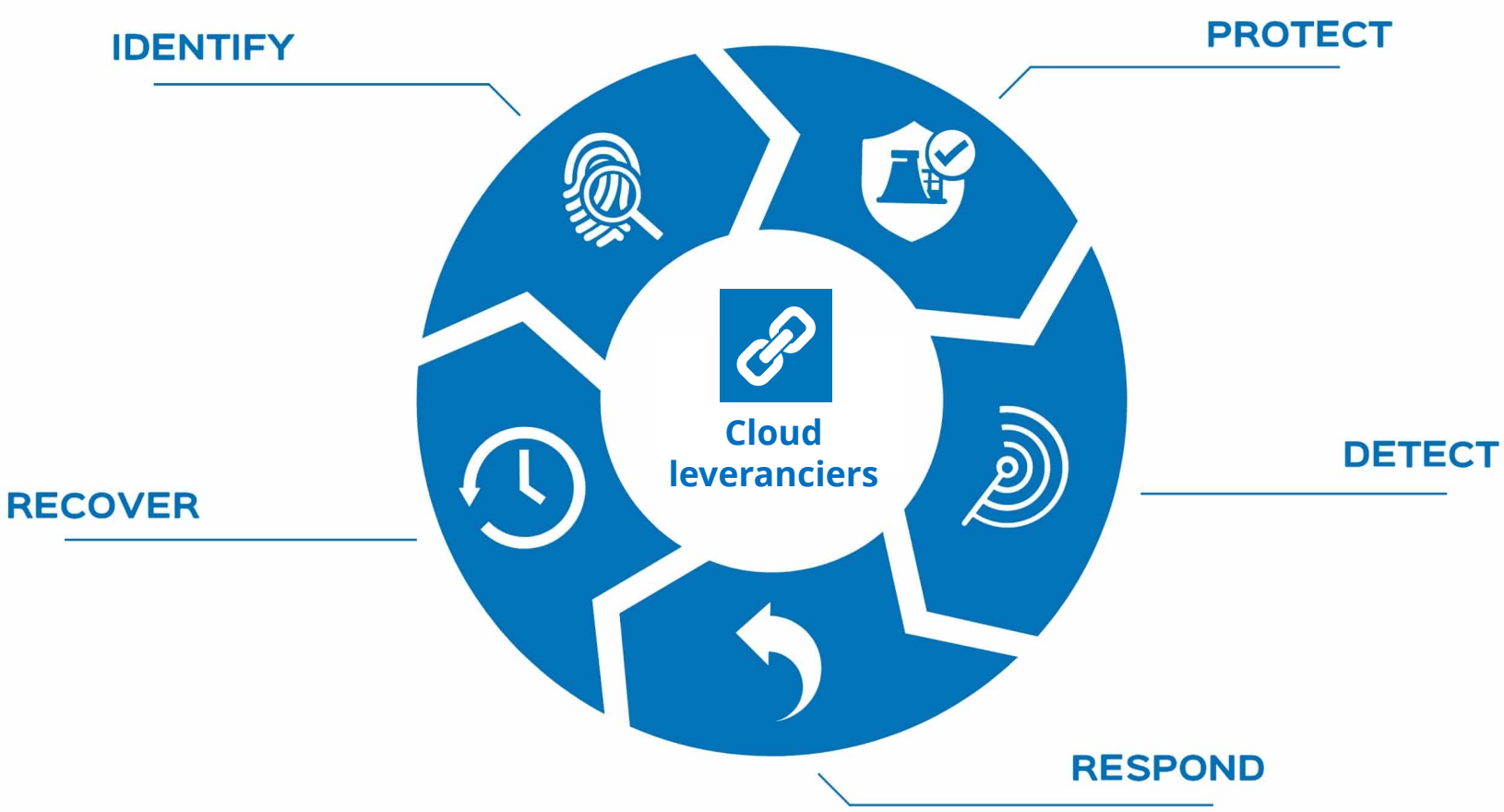
MBO Digitaal & MBO Raad
Versie 1.7
2 september 2022

mbo digitaal

Programma Cyberveiligheid mbo

mbo digitaal

Programma Cyberveiligheid mbo



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

Identificeren van dreigingen en risico's (*identify*)

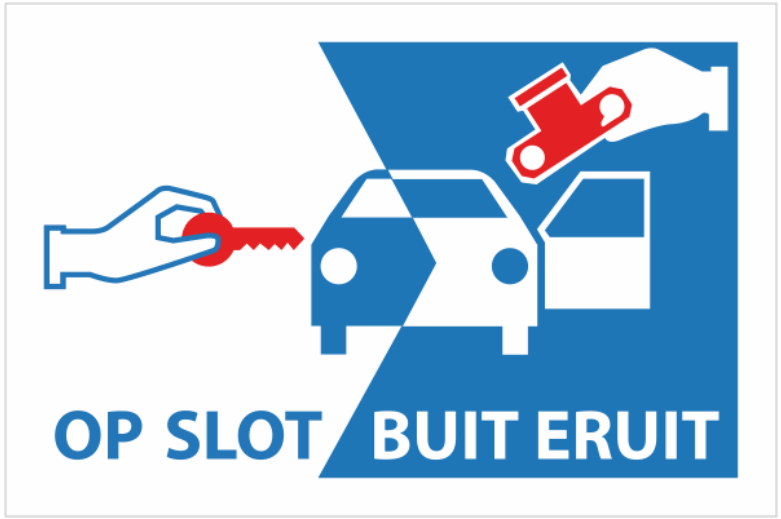
- Op welke gebieden lopen we risico's?
  - Cyberdreigingsbeeld (SURF)
  - Standaardaanpak risicomanagement
- Hoe staat de organisatie/sector ervoor?
  - Normen/toetsingskaders IB en P
  - Benchmark IBP / peerreview
  - Externe IT-audits
  - Enquetes (awareness bijv)
- Wat staat ons te doen?
  - De hele organisatie aan zet!
  - Governance > bestuur
  - Processen > proceseigenaren
  - Technische weerbaarheid > IT

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

mbo digitaal

Beschermen tegen cyberrisico's (*protect*)

- Awareness: metingen, trainingen en campagnes (phishing bijv)
- Technische maatregelen (MFA, offline backups bijv)
- Van ransomware naar exfiltratie: zorg dat er niks te halen is!
  - Stop met fileshares (de G: schijf)
  - Dataminimalisatie (ook vanwege AVG)
  - Geen schaduwadministraties



mbo digitaal

Detecteren van onregelmatigheden (*detect*)

SURFsoc

- Analyseert log-bestanden
- Detecteert verdachte activiteit
- Bij enstige verdenking: contact met de instelling
- Melding SURFcert > delen binnen de hele sector

- Aansluitkosten (€50.000) vergoed vanuit subsidie
- Doorontwikkeling: opvolging meldingen > 24/7 (?)

mbo digitaal

Reageren op incidenten (*respond*)

- Inzicht gebruik applicaties mbo-breed
  - Ontwikkeling mbo-brede applicatiecatalogus
  - Snel reageren (LOG4J bijv)
- Crisismanagement
  - standaard crisisaanpak
  - samen oefenen (cybercrisisoefening OZON bijv)
- Delen *Indicators of Attack / Indicators of Compromise*
- Centrale rol SURFcert

➢Cyberconvenant mbo

mbo digitaal

Herstellen van incidenten (*recover*)

- Cyberverzekering
- Risicopooling
- Elkaar uitwijkopties bieden
- Delen van geleerde lessen

➢Cyberconvenant mbo

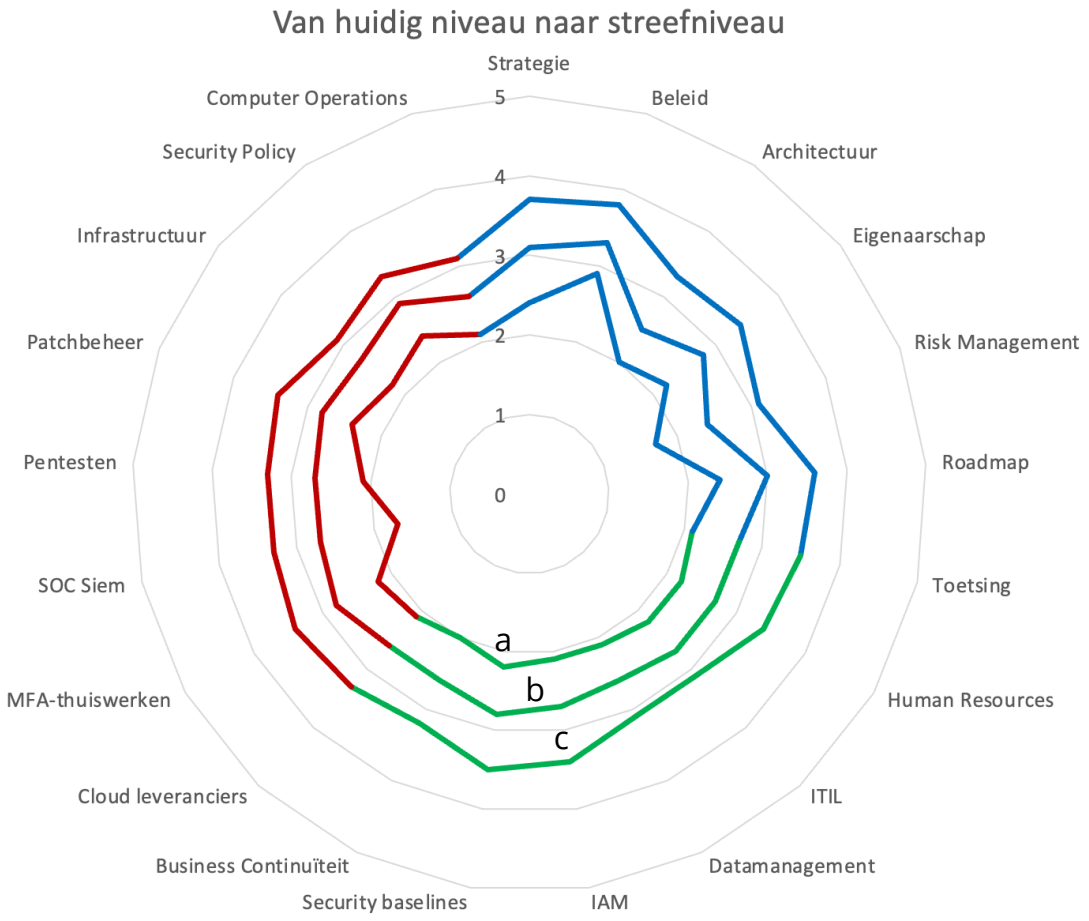
mbo digitaal

Cloudleveranciers

- Centraal beoordelen (verwerkers)overeenkomsten
- Centraal uitvoeren DPIA’s, pentests en audits
- Ontwikkelen (en gebruiken) mbo-brede applicatiecatalogus

mbo digitaal

Programma Cyberveiligheid van start met nulmetingen



Governance - Processen - Technische weerbaarheid

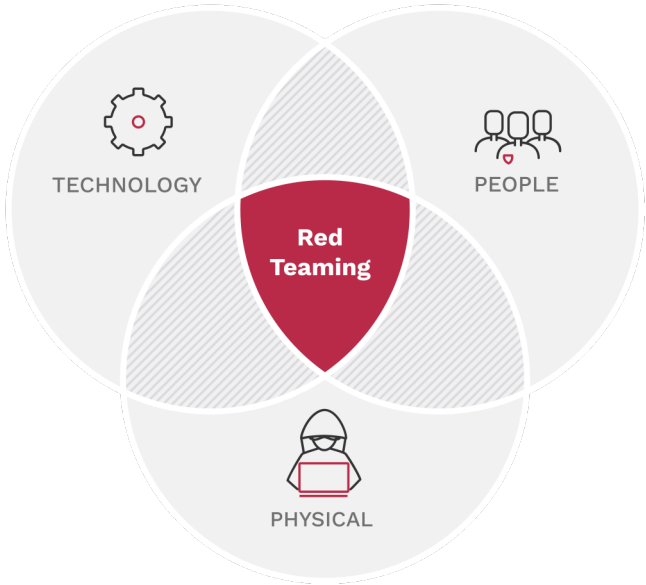
- Nulmeting Informatiebeveiliging
  - Oktober-november 2022
  - In plaats van Benchmark IBP-E
  - Met het nieuwe NBA-toetsingskader
  - 49 mbo-instellingen

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

➢ Enorme ambitie!
➢ Input voor het programma

mbo digitaal

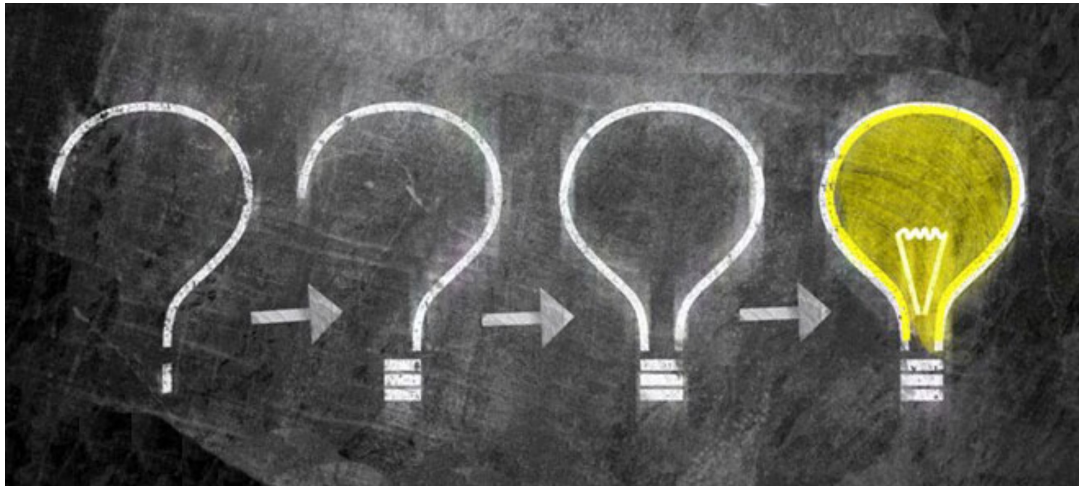
(Nul)metingen programma Cyberveiligheid



1. Volwassenheid Informatiebeveiliging
2. Governance (bestuurder en IBP-er)
   hoe is de sturing op IBP geregeld
3. Awareness (alle medewerkers)
   motivatie, capaciteit en ondersteuning om informatieveilig te (kunnen) werken
4. Crisismanagement (oefenleiders OZON)
   in hoeverre reageert de organisatie volgens verwachting bij een cybercrisis
5. Technische weerbaarheid (IV-metingen bij alle instellingen)
   in hoeverre is de instelling beschermd tegen (technische) aanvallen van buitenaf

Afsluiten met Red Teaming assessments (3 best scorende instellingen)

Vragen en discussie



Martijn Bijleveld
m.bijleveld@mbodigitaal.nl

https://mbodigitaal.nl/programma-cyberveiligheid-mbo