mbo digitaal

NETWERK
Informatiebeveiliging
en Privacy

MBO brede afspraken over beperken cyberrisico's

27 januari 2023

Over o.a. een mbo-breed cyberconvenant en het gezamenlijk dragen van cyberrisico's door een collectieve verzekering.

Martijn Bijleveld

Peter Vermeijs

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

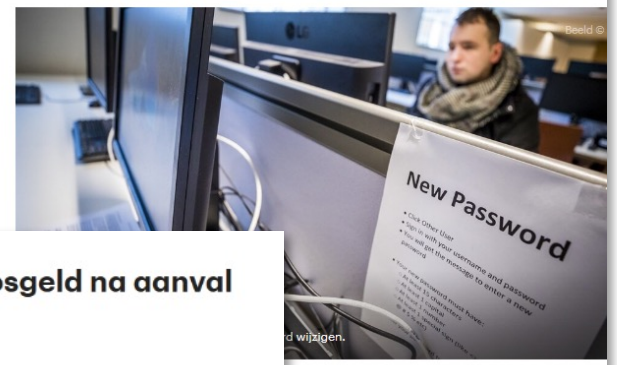
Hackers bieden op een internetforum persoonlijke gegevens van 56.000 studenten van InHolland aan. I zijn vorige maand buitgemaakt. De hack past in een groeiende trend waarbij organisaties met veel persoonsgegeve

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

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

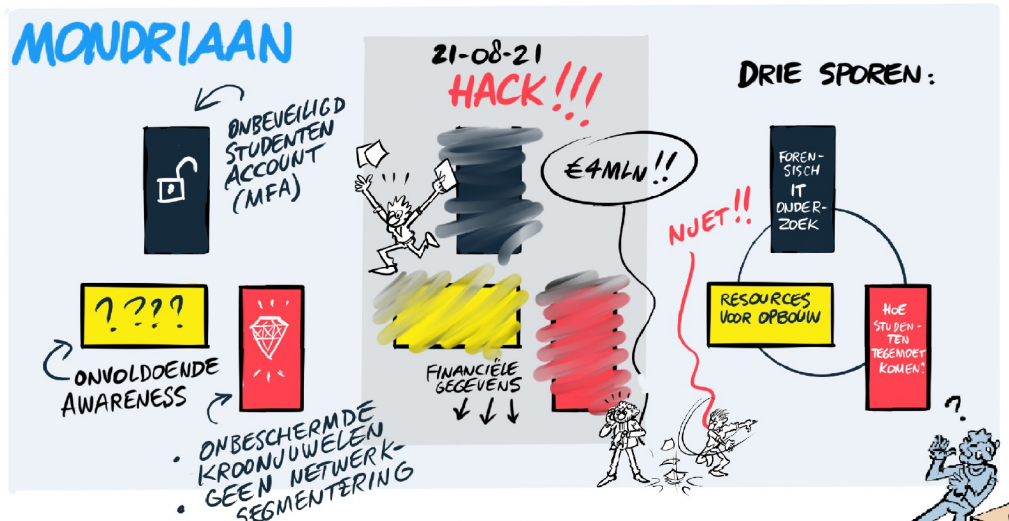
WELKOM 123

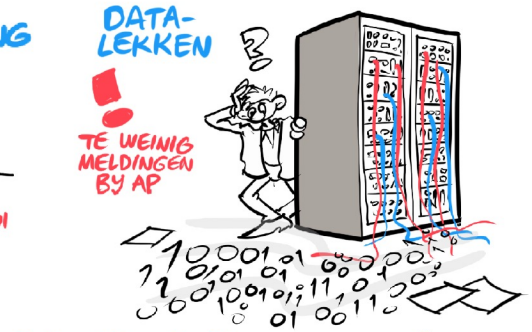
MBO-RAAD 6 DECEMBER 2021 + MINISTERIE OC&W, INSPECTIE VAN HET ONDERWIJS, AUTORITEIT PERSOONSGEGEVENS

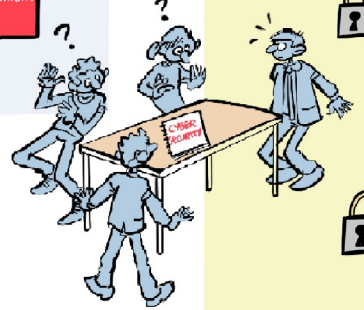
BESTUURDERSBIJEENKOMST CYBERSECURITY

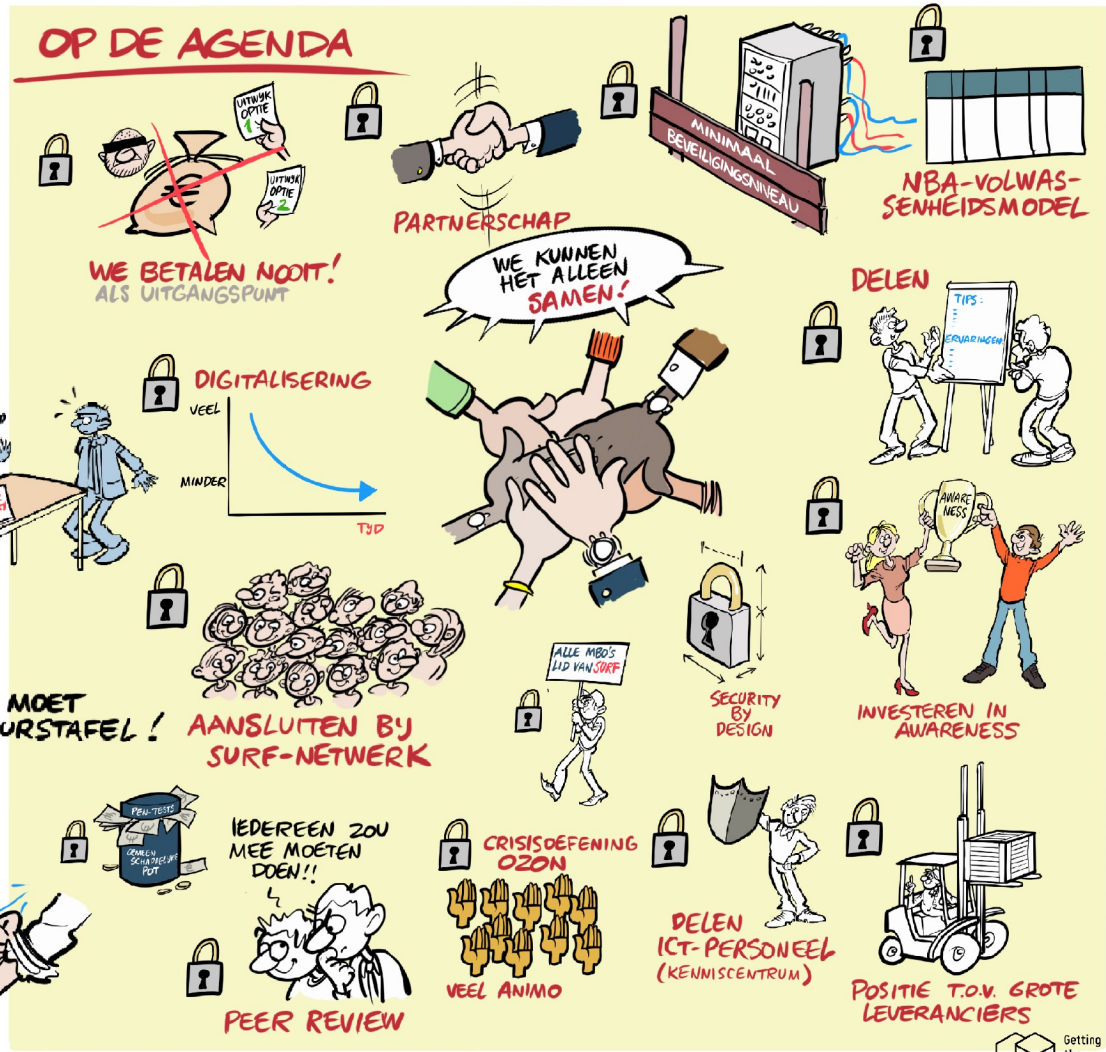
ZEER GEÏNTERESSEERD VAN WIE 38 BESTUURDER

- 69 DEELNEMERS
- 39 MBO-INSTELLINGEN



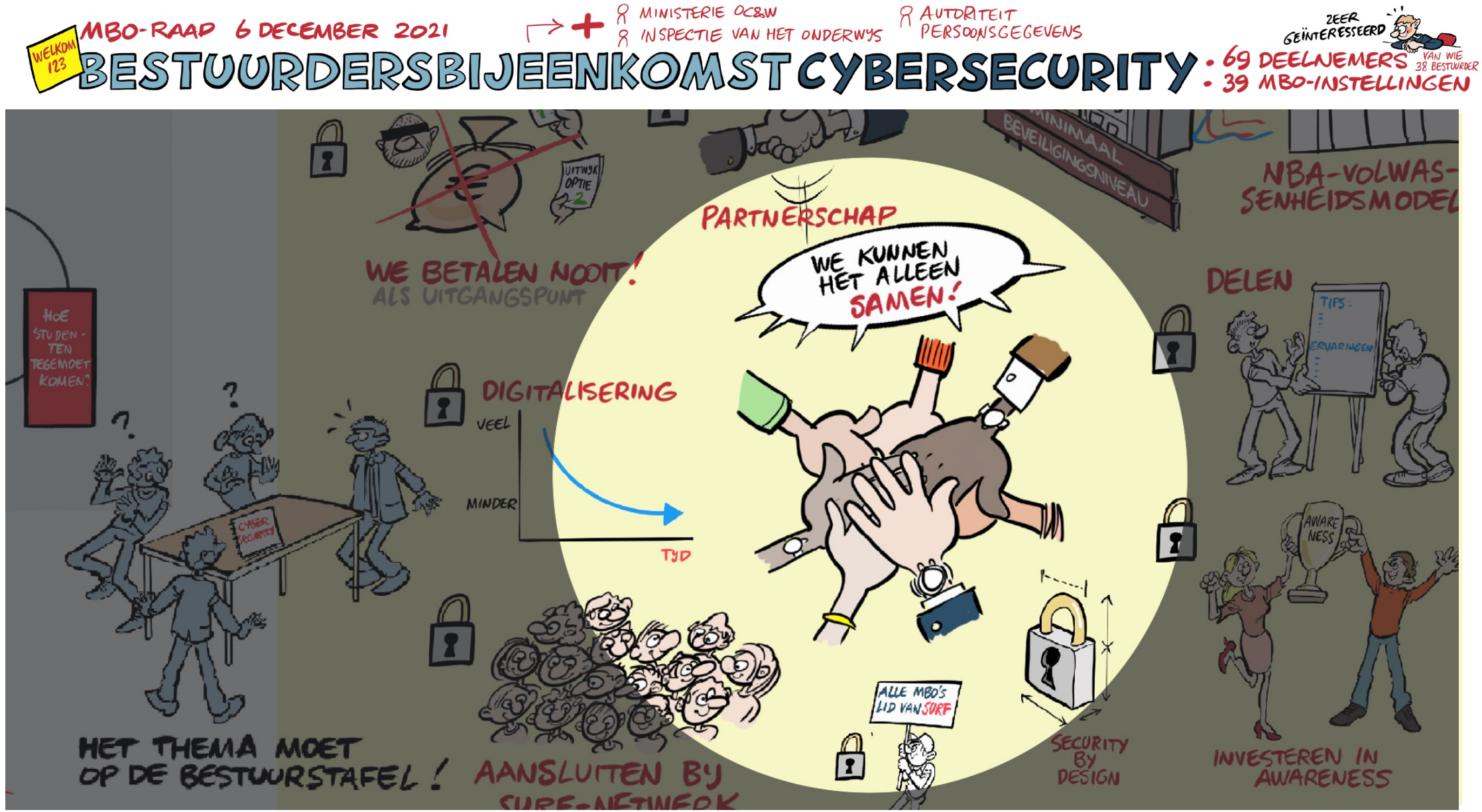






Getting the picture.

mbo digitaal



Programma Cyberveiligheid mbo

- Centrale mbo-brede aanpak
  gecoördineerd door MBO Raad / MBO Digitaal
- Afstemming met netwerk IBP via regiegroep
- 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

Waarover willen we mbo-breed afspraken maken?

1. Governance IBP in het mbo
2. Normen/toetsingskaders IB en P
3. Beheren volwassenheid via GRC-applicatie
4. Deelname benchmarks en (nul)metingen IB en P
5. Verantwoording volwassenheid via jaarlijkse rapportage
6. Crisismanagement cyberincidenten
7. Beperken impact cyberincidenten
8. Leveranciersmanagement

mbo digitaal

Waarover willen we mbo-breed afspraken maken?

- Besproken tijdens bestuurdersbijeenkomst 26-01-2023:
  - tref voorbereidingen voor een cyber convenant
  - begin februari naar Stuurgroep MBO Digitaal

Discussie:

➢ wat zijn de belangrijkste afspraken die we op bestuurlijk niveau moeten maken?

➢ en welke zaken kunnen we in het netwerk IBP + regiegroep regelen?

mbo digitaal

Governance IBP in het mbo

- Netwerk IBP in het mbo
  - Mandaat regiegroep IBP (9 mbo-instellingen)

➢ Op basis van consensus

- Wanneer nodig: formele besluitvorming
  - Stuurgroep MBO Digitaal
  - Bestuur MBO Raad
  - Regiobijeenkomsten (Bedrijfsvoering)
  - ALV ledenraadpleging

mbo digitaal

Normen/toetsingskaders IB en P

- We gebruiken de SURFaudit-toetsingskaders
  - NBA-volwassenheidsmodel IB
  - SURFaudit toetsingskader privacy
- We stelen mbo-breed, met OCW, het ambitieniveau + tijdpad vast
- We standaardiseren als basis voor samenwerken: modelaanpak
  - afspraken over interpretatie en scope van de controls
  - afspraken over risicoframeworks (bv 3 lines model en cyberdreigingsbeeld)
  - deelnemen aan audit-trainingen (objectiviteit benchmarks)
  - we delen modeldocumenten en best practices

mbo digitaal

Beheren volwassenheid via GRC-applicatie

- We gebruiken een standaard GRC-applicatie (via SURFaudit)
  - voor het bijhouden van de actuele- en de streefvolwassenheid
    - bij voorkeur als eigen stuurinstrument voor de instellings-roadmap IBP
    - inclusief de (model)documentatie/bewijslast
  - voor regelmatig aanleveren volwassenheidscores (export/koppeling)
    - ten behoeve van monitoring groei en inzetten activiteiten programma cyberveiligheid
  - voor jaarlijkse benchmarks
  - voor de externe toegang voor (peer) reviews en externe audits

mbo digitaal

Deelname benchmarks en (nul)metingen IB en P

- We leveren onze gegevens aan voor de benchmarks IB en P
- We werken mee aan de beoordeling/vaststelling van de scores
  - via peer reviews, expert reviews en externe audits
- We nemen deel aan andere enquete-instrumenten IB en P
  - Governancemeting (bestuurder en IBP-er)
    - hoe is de sturing op IBP geregeld
  - Awarenessmeting (alle medewerkers)
    - motivatie, capaciteit en ondersteuning om informatieveilig te (kunnen) werken
    - input voor programma Cyberveiligheid en Digitaal bekwaam mbo

mbo digitaal

Verantwoording volwassenheid via jaarlijkse rapportage

- We maken afspraken over vorm en inhoud van de IBP-rapportage
  - per instelling (via jaarverslag bijv)
  - sectorbreed trendrapport en verantwoording programma cyberveiligheid
  - ➢ afweging openheid <> veiligheid

mbo digitaal

Crisismanagement cyberincidenten

- We gebruiken een mbo-brede applicatiecatalogus
  - mbo-breed actueel inzicht in het gebruik van applicaties
- We maken afspraken over crisismanagement
  - kennisdeling crisisaanpak (crisisplannen bijv)
  - we zijn aangesloten bij SURFcert: alle mbo's lid van SURF
  - we delen de *Indicators of Attack* (IoA's) en *Indicators of Compromise* (IoC's) met SURFcert
    (ook als dat niet het standaardbeleid van de incident-response partij is)
  - gezamenlijk oefenen: bijv cybercrisisoefening OZON
- We spreken af (en dragen uit): wij geven niet toe aan afpersing

mbo digitaal

Beperken impact cyberincidenten

- Rondvraag binnen netwerk FG’s naar gebruik cyberverzekeringen
  - 35 geantwoord; 9 wel, 26 geen verzekering
- Het beperken van cyberrisico’s is, naast een eigen verantwoordelijkheid van de school, ook een sectorbrede aangelegenheid.
- We nemen samen het initiatief voor een cyber-calamiteitenfonds
  - voorwaarde: alleen uitkering voor beperken impact en herstel
  - alternatief: onderzoek collectieve verzekering, aanbesteed via SURF
  - acceptatie obv (gevalideerde) zelfassessments IB
- We bieden elkaar uitwijkopties
- We delen de geleerde lessen

mbo digitaal

Cloud leveranciers

- We gebruiken een mbo-brede applicatiecatalogus
  - mbo-breed actueel inzicht in het gebruik van applicaties
- We hanteren een gezamenlijke aanpak mbo-leveranciers
  - centrale afstemming over (verwerkers)overeenkomsten
  - controle op veiligheidswaarborgen (DPIA's, pentests en audits)
  - we stellen de daarvoor benodigde budgetten beschikbaar (tot 2027 vanuit de subsidie)

Hoe willen we de afspraken maken?