

WORKSHOP

Cyber risk pooling in het mbo

SAMENWERKEN AAN

CYBERVEILIGHEID

IN HET MBO



JAAR
1



PROGRAMMA
Cyberveiligheid

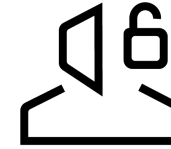


NETWERK
Informatiebeveiliging
en Privacy

MBO Raad

mbo digitaal

mbodigitaal.nl/cyberveiligheid



Cyber risk pooling in het mbo

Over het gezamenlijk dragen van cyberrisico's door een mbo-brede cyber risicopool.

Peter Vermeijs (MBO Raad)

Martijn Bijleveld (MBO Digitaal)

Bernold Nieuwesteeg (Erasmus Universiteit)

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.

de Volkskrant

Hogeschool InHolland gehackt: persoonlijke gegevens tienduizenden studenten aangeboden op internetforum

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

Laurens Verhagen 1 ma



▲ Nijmeegse studenten van de HAN. © David van Haren

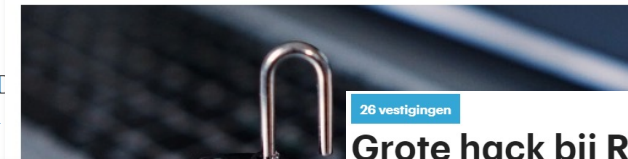
HAN: 4300 wachtwoorden gelekt, totale omvang hack nog niet bekend

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

Ransomware

Staring College betaalt losgeld na aanval met gijzelsoftware

26 februari 2021 20:59



26 vestigingen

Grote hack bij ROC Mondriaan: computers plat en bestanden ontoegankelijk

23 augustus 2021 16:29



Studenten van het ROC Mondriaan in 2021.

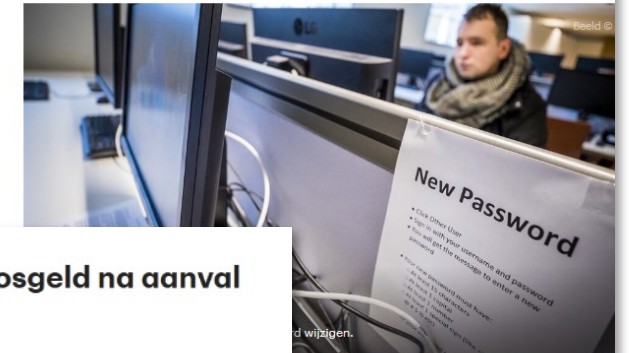
Onderwijsinstelling ROC Mondriaan in Den Haag is afgelopen weekend gehackt door criminelen. De computers liggen plat en

Grote cyberaanval

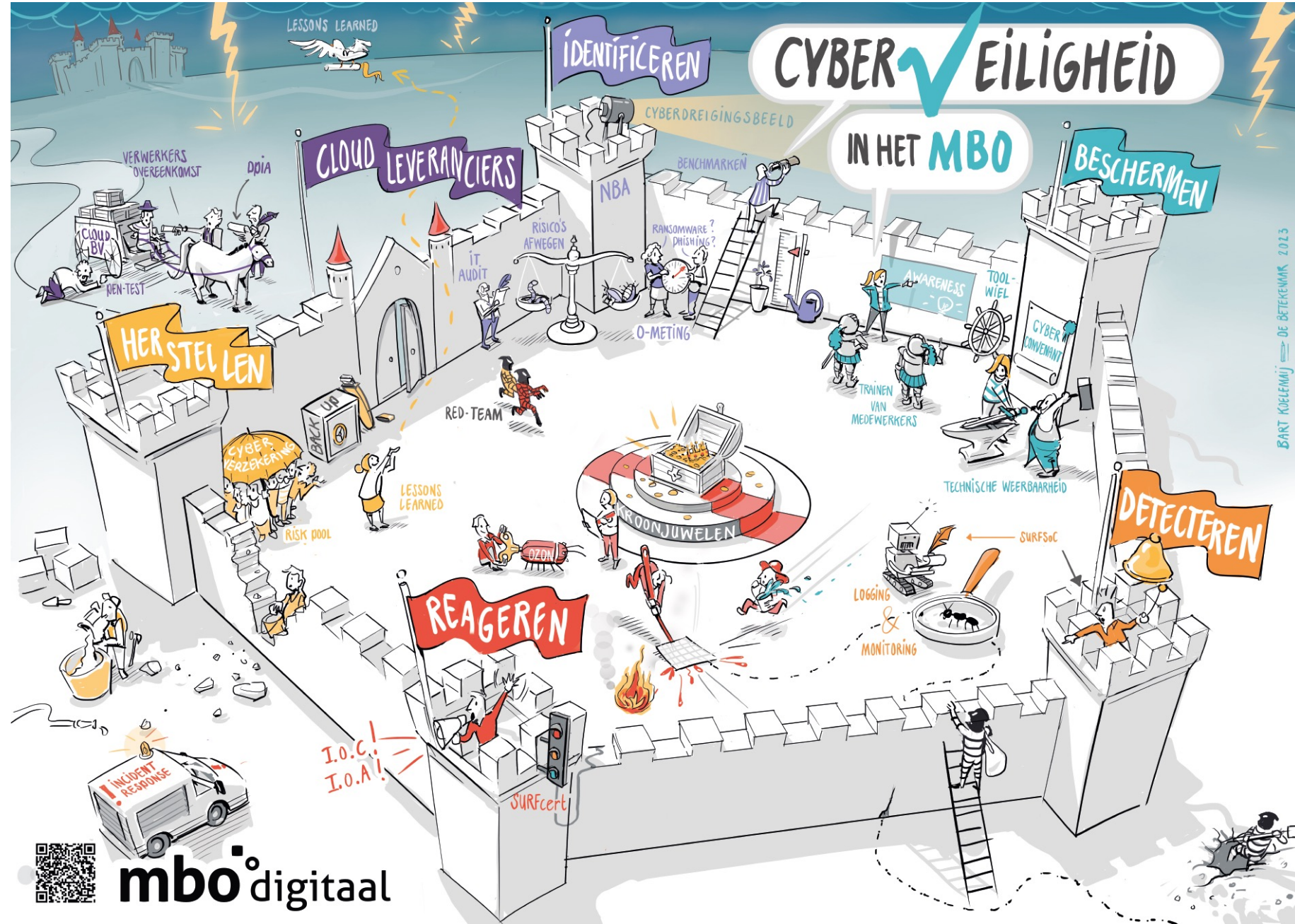
Universiteit Maastricht betaalde 197.000 euro losgeld aan hackers

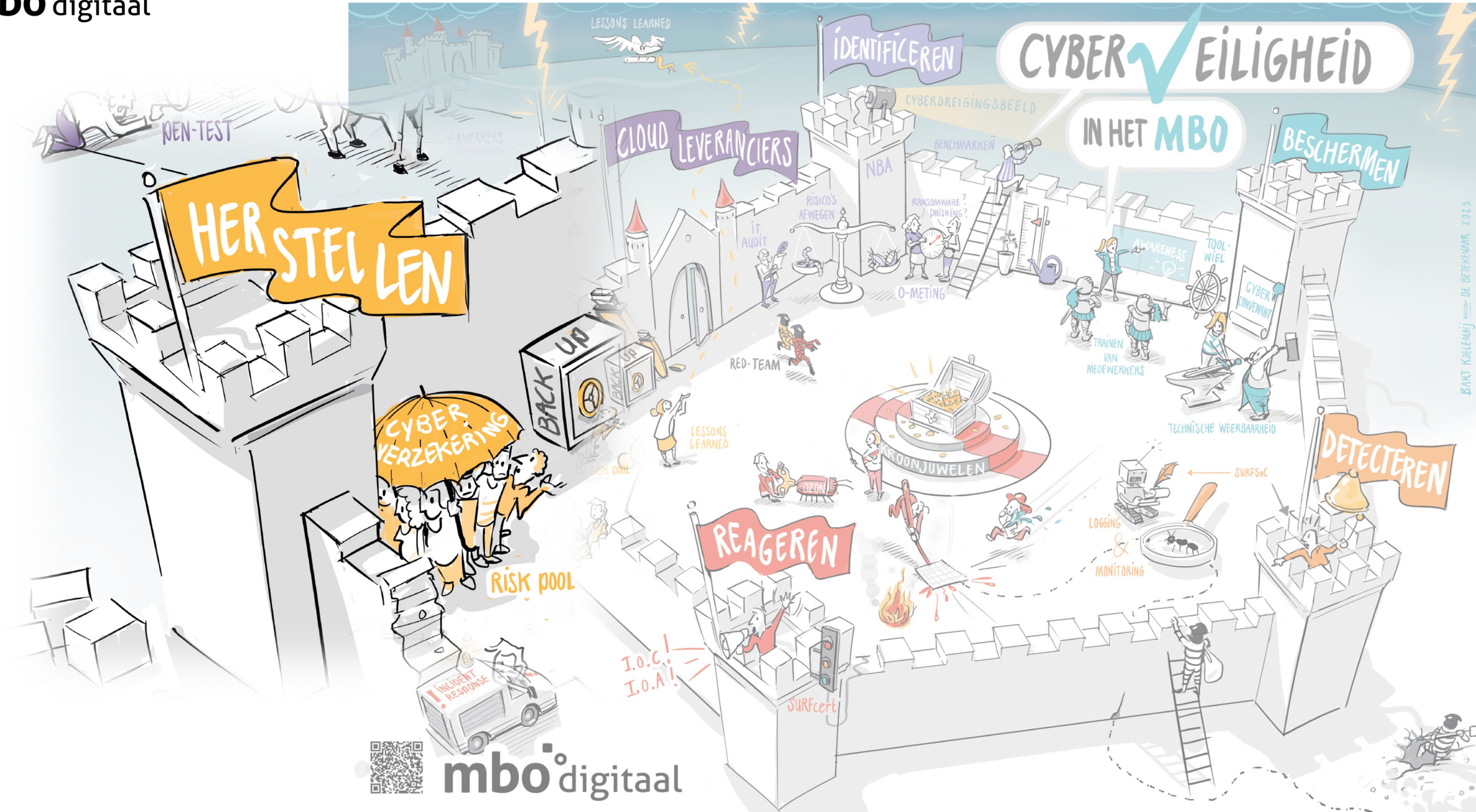
05 februari 2020 15:12

Aangepast: 05 februari 2020 20:38




heeft bijna twee ton aan losgeld betaald voor verspreide computersystemen kort voor de kerstvakantie.





Convenant cyberveiligheid mbo

- Aangenomen in de AV in juni en ondertekend in september '23
 - Afspraken over samenwerken aan cyberveiligheid
 - Governance IBP in het mbo
 - Normen/toetsingskaders IB en P
 - Volwassenheid en risicomanagement via GRC-applicatie
 - Deelname benchmarks en audits IB en P
 - Gezamenlijke optrekken met cloudleveranciers
 - **Gezamenlijke aanpak crisismanagement**
 - **Beperken impact cyberincidenten**
- 

Wat is het (cyber)risico

- Onderwijssector is sterk afhankelijk geworden van ICT
- Kans op een hack is klein en statistisch moeilijk te bepalen
- Impact is groot
 - losgeld (reken met 2% jaaromzet)
 - kosten herstel IT-omgeving
 - kosten incidentrespons
 - inkomstenderving
 - schadeclaims
 - boetes
 - reputatieschade
- We rekenen met een schadebedrag van 2,5 miljoen

Omgaan met het risico

Drie opties

1. het risico zelf dragen > aanhouden reserve
 2. het risico overdragen > cyberverzekering
 3. gezamenlijk het risico dragen > risicopool
-
- Enquete cyberverzekeringen (35 mbo-scholen)
 - 9 hebben een cyberverzekering
 - 26 dragen het risico zelf (al dan niet vrijwillig)

Ervaringen met cyberverzekeringen

- Strikte toelatingseisen
 - Grote hoeveelheid vragen en bewijsstukken
 - Niet in lijn met ons eigen IB-assessment
 - (Nog) niet haalbaar voor veel (kleine) mbo-instellingen
- Veel uitsluitende bepalingen
 - Als schade (deels) toerekenbaar is aan de mbo-instelling
 - Bij wijdverspreide incidenten wordt de uitkering beperkt
- Hoog eigen risico
- Hoge premie
- Twijfel: komt het wel tot een uitkering bij een incident...

Onderzoek vanuit programma Cyberveiligheid

- Zijn er mogelijkheden voor een collectieve cyberverzekering?
 - Toelating op basis van ons toetsingskader IB (NBA/NOREA-model)
 - Inspraak in de voorwaarden (bijvoorbeeld niet-betalen aan criminelen)
 - Ruimte voor het principe dat de sterkste schouders de zwaarste lasten dragen
 - Voorlopige acceptatie van instellingen die nog niet voldoen (op basis van een risico-analyse en een plan van aanpak)
 - Vraag neergelegd bij twee makelaars in cyberverzekeringen
 1. Kansloos: verzekeraar doet altijd een individuele beoordeling van het risico.
 2. Eventueel mogelijk: als alle 55 instellingen meedoen en dit extra risico kan worden doorberekend in de collectieve premie. Het collectief heeft er baat bij om de zwakkere instellingen te helpen om de premie beheersbaar te houden.
- Misschien kunnen we het beter in eigen hand houden?

Gezamenlijk risico's dragen via een cyber risk pool

- Onderling delen van cyberrisico's zonder tussenkomst van een verzekeraar
- Op basis van een contractuele afspraak staan de instellingen garant voor elkaar
- De leden leveren alleen een financiële bijdrage als er daadwerkelijk schade is
- Schade wordt vastgesteld door een onafhankelijke schade-afhandelaar
- Het schadebedrag wordt gedeeld door de leden van de risicopool

De voordelen van een risicopool

- Kent een ingebouwde prikkel voor samenwerken en elkaar helpen op het gebied van cyberveiligheid
- Stimuleert wederzijdse monitoring, kennisdeling en bewustwording
- Benchmarken en externe security-audits krijgen nog meer betekenis
- De sterkste schouders kunnen de zwaarste lasten dragen
- De toelatingseisen bepalen we als sector zelf (toetsingskader IB)
- Incidentrespons en schade-afhandeling kan mbo-breed georganiseerd
- De uitgespaarde verzekeringspremies kunnen door de scholen worden geïnvesteerd in mitigerende maatregelen

Voorwaarden voor een succesvolle risicopool

- De leden moeten elkaar kennen en vertrouwen
 - De leden leggen naar elkaar verantwoording af over risico's en maatregelen (via self-assessments en externe audits)
 - Leden zijn bereid elkaar te helpen om de weerbaarheid te verhogen
 - De pool heeft een zekere omvang nodig om de schade te kunnen opvangen
- De mbo-sector voldoet aan alle voorwaarden voor een succesvolle risicopool!

Uitwerking: het aandeel in de pool

- Scenario's
 1. op basis van het IB-volwassenheidsniveau van de instelling
 - hogere volwassenheid leidt tot een lager risico en daarmee een lager aandeel in de pool
 2. op basis van de gekozen dekking en het eigen risico
 - instellingen die kiezen voor een beperktere dekking dragen in het collectief minder bij aan het risico wat zich vertaalt in een geringer aandeel
 3. op basis van het aantal ingeschreven studenten
 - een gebruikelijke manier voor mbo-instellingen om bij te dragen aan gemeenschappelijke voorzieningen
 4. de schade wordt gelijk verdeeld, ongeacht de grootte of het risico van de instelling
- Ook een combinatie is mogelijk, bijvoorbeeld scenario 1 en 3

Uitwerking: incidentrespons

- Gemeenschappelijk organiseren van processen
 - SOC, CERT, cyber-forensics, incidentrespons, schade-expertise, het bieden van uitwijkopties en herstel van de schade
- Niet meer gebonden aan een verzekeraar
- Geen individuele retainer-overeenkomsten meer
- Incidentrespons en schade-afhandeling gezamenlijk aanbesteden
 - betere informatie-uitwisseling
 - sneller reageren
 - doelmatig: kostenbesparing

Uitwerking: schade-afhandeling

- Onafhankelijke schade-afhandelaar
 - schade beperken: biedt tegenwicht aan partijen voor incidentrespons
 - doelmatige besteding van middelen
 - bewaakt dat getroffen instelling niet in een betere positie komt dan daarvoor
- Cruciaal voor het vertrouwen van de leden in de risicopool

Uitwerking: financieel

- Financiële ruimte van de risicopool
 - Uitgaande van de gemiddelde jaarlijkse (!) verzekeringspremie:
55 instellingen x € 60.000 = 3,3 miljoen euro in een (virtueel) fonds
 - afhankelijk van eventuele schade en andere kosten wordt dit aangevuld
 - het bestuur van de risicopool besluit hierover
- Vaste kosten
 - retainer voor schade-afhandeling en incidentrespons (=verschuiving van kosten)
 - bureaunkosten (bijv. als dienst SURF)
 - via jaarlijkse bijdrage van de leden

Maar we benoemen hier ook de olifant...

- De leden moeten comfortabel zijn met een verdeelsleutel (aandeel in de pool) die niet 100% overeenkomt met het werkelijke individuele risico. Je loopt risico voor je collega-instelling die het wellicht minder goed voor elkaar heeft dan jij.
 - Er is een (hypothetisch) risico dat een groot deel, of zelfs alle instellingen tegelijkertijd getroffen worden en de risicopool zijn werking verliest.
- Is dit in een verzekeringsscenario beter geregeld?



Opstarten van een risicopool (1)

1. Bepaal wat wel/niet wordt gedekt
 - bijvoorbeeld incidentrespons, herstel, maar niet de betaling aan criminelen
2. Maximale uitkering en eigen risico
 - bijvoorbeeld 2,5 miljoen in combinatie met een hoog eigen risico (€100.000)
3. Toelatingseisen
 - bijvoorbeeld de aansluiting op een SOC en een minimale score op (delen) van het toetsingskader
4. Verdeling van het aandeel in de pool
 - iedere deelnemer voor een gelijk deel, of op basis van studentenaantal, volwassenheidsscore (of een combinatie van deze factoren)

Opstarten van een risicopool (2)

5. Selecteer een schadeafhandelaar
 - het contract met de gespecialiseerde onafhankelijke schadeafhandelaar wordt door de pool aanbesteed
6. Organiseer de incidentrespons-keten
 - de pool maakt bij voorkeur gebruik van een gemeenschappelijke SOC en CERT-functie, op basis waarvan een incident respons partij wordt gecontracteerd (voor zover deze functie niet door de schadeafhandelaar wordt verzorgd)
7. Organiseer een bureau voor de administratieve taken
 - mogelijk kan SURF dit als dienst aanbieden
8. Werk de statuten en het contract uit
9. Formeer het bestuur van de risicopool

Conclusies en vervolgstappen

- 1. We hebben een goede voedingsbodem binnen het mbo
- 2. Risicopooling is veel meer is dan enkel het afdekken van risico's: het is een extra drijfveer in de samenwerking en kennisdeling tussen de mbo-scholen op het gebied van cyberweerbaarheid
- 3. Vertrouwen in elkaar cruciaal. Dat moet worden onderbouwd door middel van externe security-audits, in combinatie met het toepassen van de met elkaar afgesproken minimale set aan maatregelen op het gebied van cyberweerbaarheid.
- 4. Veel moet nog worden uitgewerkt, maar voordat we verdergaan:
 - Informatierondes voor bestuurders en toezichthouders
 - Andere suggesties?