mbo digitaal

CYBERVEILIGHEID IN HET MBO

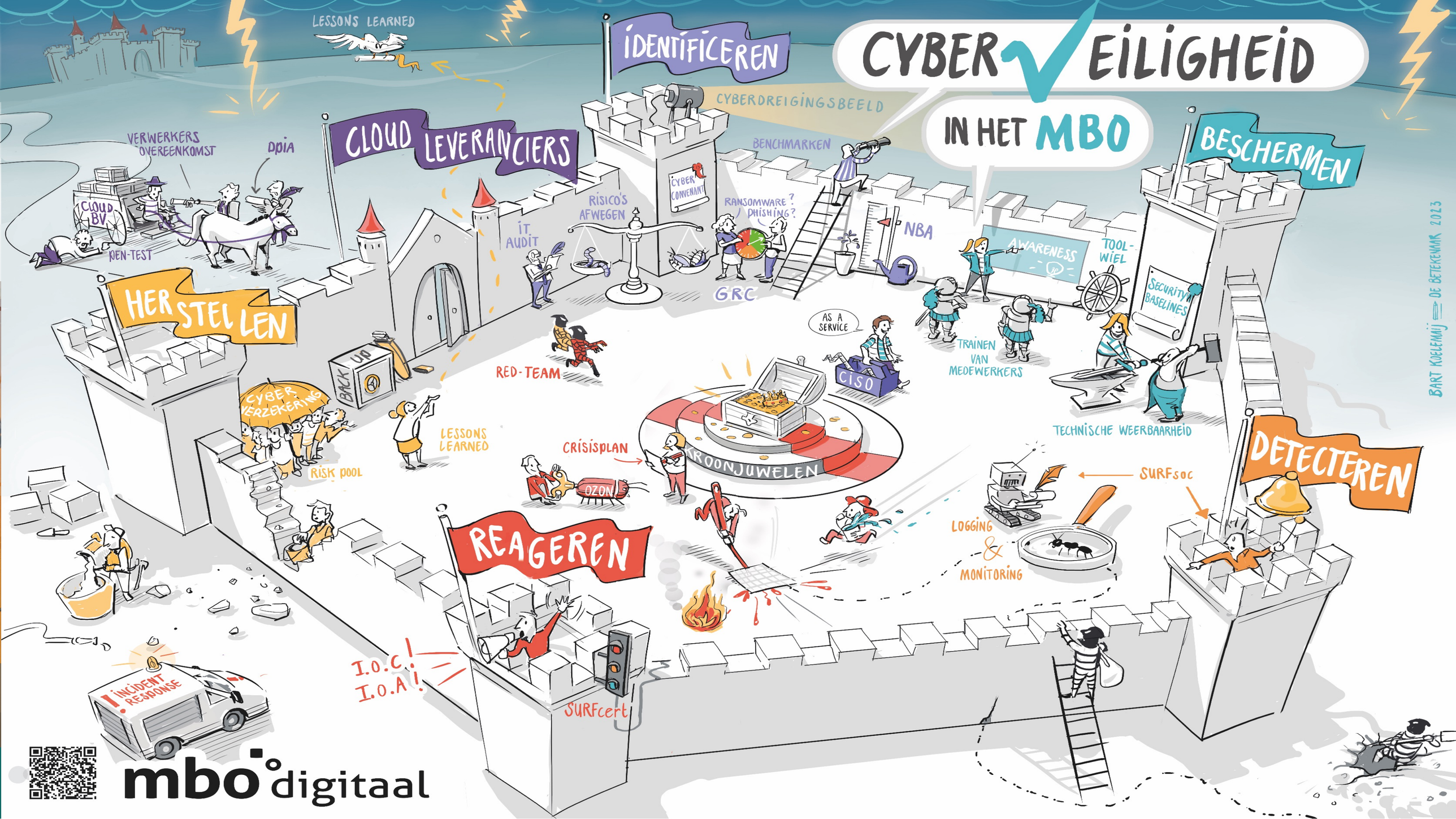
Workshop CISO as a Service

Verbeter de cyberweerbaarheid van jouw instelling

Henry Meutstege

8 maart 2024

V1


LESSONS LEARNED
IDENTIFICEREN
CYBER VEILIGHEID
IN HET MBO
CYBERDREIGINGSBEELD
BENCHMARKEN
CLOUD LEVERANCIERS
VERWERKERS OVEREENKOMST
DPIA
CLOUD BV
KEN-TEST
IT AUDIT
RISICO'S AFWEGEN
CYBER CONVENANT
RANSOMWARE? PHISHING?
GRC
NBA
BESCHERMEN
AWARENESS
TOOL-WIEL
SECURITY BASELINES
TRAINEN VAN MEDEWERKERS
TECHNISCHE WEERBAARHEID
HERSTELLEN
BACK UP
CYBER-VERZEKERING
RISK POOL
LESSONS LEARNED
RED-TEAM
AS A SERVICE
CISO
CRISISPLAN
OZON
KROONJUWELEN
REAGEREN
I.O.C!
I.O.A!
SURFcert
INCIDENT RESPONSE
SURFsoc
LOGGING & MONITORING
DETECTEREN
BART KOELEMIJ DE BETEKENMR 2023
mbo digitaal

mbo digitaal

Doelstelling CISO as a Service

- Verbeteren digitale weerbaarheid instelling
- NBA model/SURFaudit Toetsingskader als leidraad
- Governance, Processen en Technische weerbaarheid
- Bijvoorbeeld:
  - Helpen bij schrijven van beleid
  - Helpen bij de NBA toetsing (voor 15 maart 2024)
  - Risico gebaseerd plan maken (jaarplan, roadmap)
  - Kwetsbaarheden in beeld brengen
  - SOC/SIEM bespreken
- Niet vrijblijvend…
  - Commitment van bestuur & management (en daar zal de CISO bij helpen…)
  - Kost ook inspanning en geld van instelling zelf
  - Kennis wordt gedeeld met overige instellingen

mbo digitaal

CISO as a Service....

Verbeteren digitale weerbaarheid

mbo digitaal

Je kunt als instelling kiezen.....

Menu Kaart

Voorgerecht

Intake

(met CVB en IBP contactpersoon)

Nul meting

(obv SURF audit toetsingskader)

Hoofdgerecht

Governance

Processen

Technische Weerbaarheid

Nagerecht

Resultaten

Input jaarplan

Gerechten

- Governance:
  - Van strategie tot beleid, inclusief risicomanagement en eigenaarschap
  - Is er een jaarplan/roadmap om informatiebeveiliging en privacy te verbeteren
  - Vindt er periodiek een (formele) toetsing plaats
- Processen:
  - Het bewustzijn binnen de instelling
  - Zijn de basis beheerprocessen op orde (ITIL)
  - Zijn de systemen en de data geclassificeerd?
  - Zijn de personeel procedures in lijn met de gewenste veiligheid?
  - Hoe is het toegangsbeheer geregeld (fysiek en logisch).
  - Wat zijn de afspraken met de leveranciers (incl. cloud leveranciers).
  - Is Bedrijfscontinuïteit en crisismanagement ingericht.
- Technische weerbaarheid van de instelling
  - Hoe zijn de operationele procedures ingericht
  - Hoe is het netwerk beveiligd
  - Hoe zijn de werkplekken beveiligd
  - Hoe worden kwetsbaarheden gedetecteerd en verholpen
  - Is er een patchbeleid
  - Is monitoring en logging ingeregeld, bij voorkeur met ondersteuning van een SOC/SIEM dienst?
  - Zijn er backup en restore procedures?
  - Vindt er periodiek een technische toets plaats door het uitvoeren van een penetratie test of een red team test?

Aanvraagproces en toedeling

- Verzoek indienen ter ondersteuning bij programma Cyber Veiligheid

De criteria voor toedeling:

- De risicoanalyse en de ernst van de dreiging; de instelling waar de hoogste risico's worden gezien krijgen voorrang. Ook de uitkomsten van eerder uitgevoerde nulmeting wordt hierin meegewogen
- De betrokkenheid van de benodigde stakeholders van de instelling (bestuur, ICT). De instelling waar er een hoge mate van betrokkenheid blijkt krijgt voorrang
- Is de instelling in staat om de ondersteuning uiteindelijk te borgen in de eigen organisatie. De mate waarin dit mogelijk lijkt wordt meegewogen
- Is de instelling duidelijk bereid de geleerde lessen te delen met de overige mbo-instellingen. Daar waar de bereidheid om kennis te delen hoog is, krijgt de instelling voorrang.

Dit resulteert in een Opdrachtomschrijving met de op te pakken thema's, de afgesproken doorlooptijd en de verdere contractuele voorwaarden. Belangrijk is daarbij ook de borging van de kennis bij de deelnemende instelling.

mbo digitaal Pilot

SVO VAKOPLEIDING FOOD

da Vinci college

MBO UTRECHT

SINTLUCAS VAKSCHOOL VOOR CREATIEF TALENT

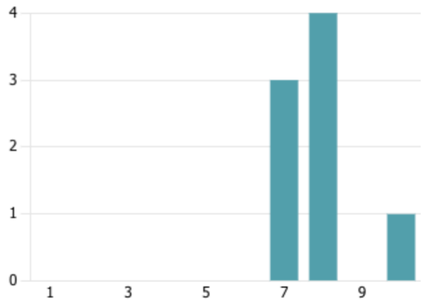
Rivor

MA Mediacollege Amsterdam

Resultaten Pilot

Tevredenheid

7.88
Gemiddelde beoordeling



Bijdrage aan cyber weerbaarheid

Niet	0
Weinig	1
Voldoende	3
Veel	3
Zeer veel	1

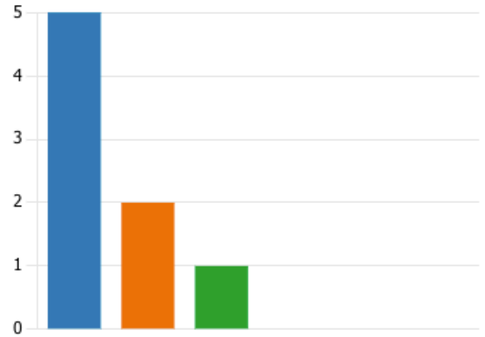
- Invullen NBA Kader
- Voorbereiden en uitvoeren NOZON
- Ciso is prominenter op de agenda gekomen
- Awareness bij MT en CvB verhoogd
- (vak)kennis en daarbij het vergelijk met de andere scholen

Uurtarief

50-75	2
75-100	5
100-125	1
125-150	0

uur per week

0 tot 4 uur	5
4 tot 8 uur	2
8 tot 16 uur	1
16 tot 24 uur	0
24 tot 32 uur	0
32 tot 40 uur	0



Wil je doorgaan met de dienst?

Ja, graag	0
Nee, bedankt	2
Graag overleg hierover	6

Wat waren de belangrijkste lessen?

- De scholen onderling (nog) meer in verbinding brengen (kwam meermaals terug!)
- Op termijn meer inzet op specifieke thema’s en onderwerpen
- Nog meer aandacht bij management en CvB verzorgen

En hoe nu verder….

Samen met SURF bezig om het onder te brengen bij het Security Expertise Centrum. Maar dat kost tijd

Pilot omzetten in een dienst vanuit Programma Cyberveiligheid, echter niet meer gratis. Tarief wordt onderwerp van gesprek. Zal mogelijk deels door programma gesubsidieerd worden.

Inzet op uren per week (bij voorkeur minimaal 8 uur per week, om toegevoegde waarde te borgen).

Inzet op specifieke opdracht, met een vooraf afgesproken resultaat (bijvoorbeeld Schrijf een beleidsstuk, Stel een advies op, Bespreek eigenaarschap met de business, etc.)

mbo digitaal Is er behoefte aan CISO as a Service??