mbo digitaal

NETWERK
Informatiebeveiliging
en Privacy

PROGRAMMA
Cyberveiligheid

Terugkoppeling Cyberveiligheid mbo

Online gebruikersdag 9 december 2024

Voortgang programma

- **Security audits**
- **Technische weerbaarheid**
- **SURFsoc Next Generation**
- **Incidentrespons**
- **Cyberrisicopool**
- **Cloudleveranciers**

Bevindingen vanuit de eerste security audits en een bruggetje naar IAM

Martijn Bijleveld

Adviseur IBP

Programmamanager Cyberveiligheid mbo

MBO Digitaal

mbo digitaal

mbo digitaal

PROGRAMMA
Cyberveiligheid

mbo digitaal

CYBERVEILIGHEID IN HET MBO

LESSONS LEARNED

IDENTIFICEREN

CYBERDREIGINGSBEELD

APPLICATIECATALOGUS

VERWERKERS OVEREENKOMST

DPIA

CLOUD BV

CLOUD LEVERANCIERS

PENTEST

HERSTELLEN

SECURITY-AUDIT

RISICO'S AFWEGEN

CYBER CONVENANT

BENCHMARKEN

RANSOMWARE? PHISHING?

GRC

NBA

AWARENESS

TOOL-WIEL

POLICY TEMPLATES

SECURITY BASELINES

BESCHERMEN

OVERKOEPELEND OVERLEG

UNL

VH

MBO RAAD

OCW

SURF

AS A SERVICE

CISO

TRAINING

KWETSBAARHEDEN?

TECHNISCHE WEERBAARHEID

BACK UP

RED-TEAM

CYBER-RISICODOOR

LESSONS LEARNED

CRISISPLAN

OZON

KROONJUWELEN

SURFsoc

LOGGING & MONITORING

DETECTEREN

REAGEREN

I.O.C.!

I.O.A.!

SURFcert

INCIDENT RESPONSE

BART KOELEMIJ DE BETEKENAAR 2024

mbo digitaal

PROGRAMMA Cyberveiligheid

mbo digitaal

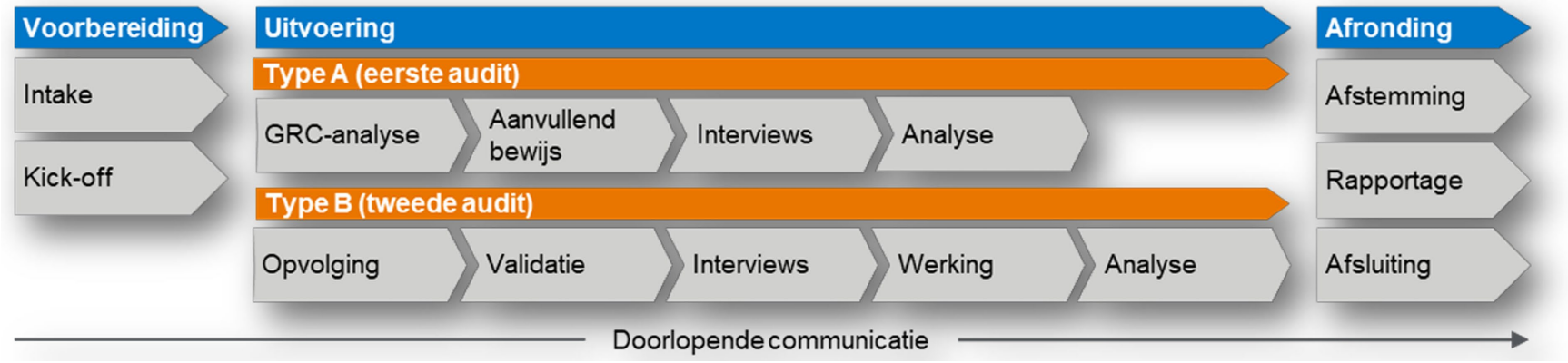
Security audits

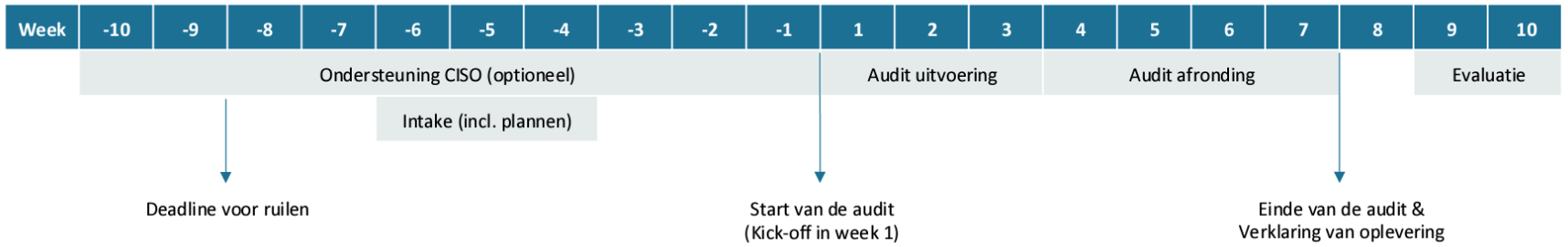
- Aanbesteding geslaagd, gegund aan Deloitte
- Alle mbo-scholen krijgen tot 2027 twee security audits
  - Eerste audit toetst opzet en bestaan, heeft een opbouwend karakter
  - Tweede audit (1,5 jaar later): volledige audit, ook de werking wordt onderzocht
- Alle 106 audits zijn ingepland
- Op basis van SURFaudit toetsingskader IB (=NBA-model)
  - Start met zelfassessment
  - Documentatie en onderbouwing in GRC-applicatie (TrustBound)
  - Ondersteuning via programma Cyberveiligheid
  - Beoordeling bewijslast door Deloitte, uitvoeren interviews
  - Rapportage door Deloitte en bespreking met management
  - Adviezen/handreikingen voor tweede audit

Week	Weeknummer	Numm	Instelling
30-12-2024	1		#N/B
06-01-2025	2	7	Curio
13-01-2025	3	23	MBO Menso Alting
20-01-2025	4	47	Talland College
27-01-2025	5	28	Noorderpoort
03-02-2025	6	20	Lentiz Onderwijsgroep
10-02-2025	7	35	ROC Ter AA
	7	18	Koning Willem I College
17-02-2025	8		#N/B
24-02-2025	9		#N/B
03-03-2025	10	19	Landstede mbo
10-03-2025	11	48	VISTA college
17-03-2025	12	24	MBO Utrecht
24-03-2025	13	43	STC
31-03-2025	14	8	Da Vinci College
07-04-2025	15	12	Gilde Opleidingen
14-04-2025	16	37	ROC van Amsterdam/Flevola
21-04-2025	17	44	Zadkine
	17	13	Graafschap College
28-04-2025	18		#N/B
05-05-2025	19		#N/B
12-05-2025	20	46	SVO vakopleiding food
19-05-2025	21	33	ROC Nova College
26-05-2025	22	50	Yuverta
02-06-2025	23	51	Zone.college
09-06-2025	24	31	ROC Mondriaan
16-06-2025	25	15	Grafisch Lyceum Utrecht

mbo digitaal

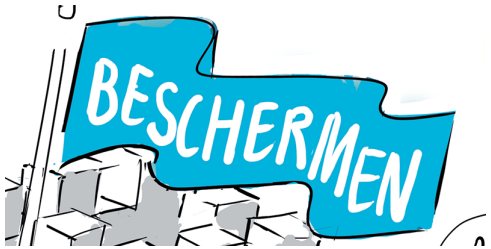
Security audits





mbo digitaal

Technische weerbaarheid

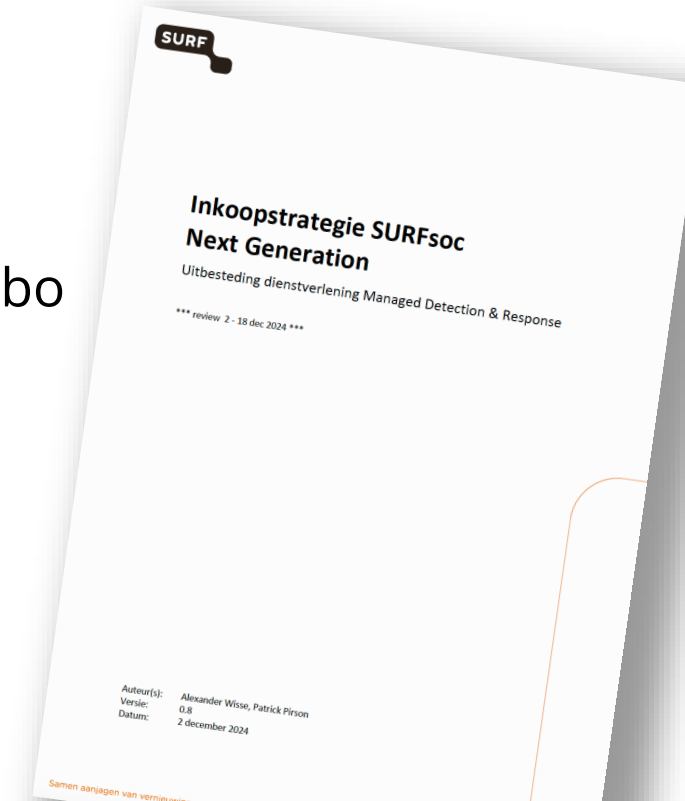


- Werkbezoeken technische weerbaarheid
  - Bijna alle mbo-instellingen zijn bezocht
  - Trendrapport: input voor programma cyberveiligheid
- Van check tot hack
  - Een 6-gangen menu met kwetsbaarhedenscans
  - Samenwerking met SURF en externe (ethisch) hackers
  - Tien mbo-instellingen nemen deel
  - Proof of the pudding: red-teaming voor 3 mbo-instellingen
- Pentesten
  - Aanbesteding in SURF-verband afgerond, zes leveranciers
  - Alle mbo-instellingen krijgen 2 gratis pentesten vanuit subsidie
  - Inhoud en scope zelf te definiëren (met ondersteuning)

mbo digitaal

SURFsoc Next Generation

- SOC = security operations center
- Pro-actief monitoren van security events in systemen en netwerken
- Aansluitkosten gesubsidieerd vanuit het programma
  - 22 instellingen gebruiken SURFsoc
  - 3 instellingen bezig met implementatie
- Nieuw PvE voor nieuwe aanbesteding SOC-diensten
  - Vanuit programma meegewerkt aan PvE: passend bij het mbo
  - Nieuwe dienst is begin 2026 beschikbaar
  - Geen nieuwe implementaties SURFsoc tot 2026
  - Inkoopstrategie is gedeeld met de leden
- Informatierondes door SURF en ons programma


SURF

Inkoopstrategie SURFsoc Next Generation

Uitbesteding dienstverlening Managed Detection & Response

*** review 2 - 18 dec 2024 ***

Auteur(s): Alexander Wisse, Patrick Pirson
Versie: 0.8
Datum: 2 december 2024

mbo digitaal

Gezamenlijke incidentrespons

- Snel reageren bij een cyberincident
- Expertise: digital forensics en incident respons (DFIR)
- Beschikbaarheid- en prijsafspraken via retainer-overeenkomst
- Kunnen we dit mbo-breed organiseren?
  - Schaalvoordelen
  - Verbetert de informatiepositie van SURFcert
  - …en daarmee de hele onderwijssector
- Samen met SURF de marktverkenning gestart

mbo digitaal

Opstarten cyberrisicopool

mbo digitaal

Opstarten cyberrisicopool

- Eind 2023 akkoord en opdracht dit verder uit te werken
  - Rechtsvorm (coöperatie) en organisatorische inbedding
  - Financiële constructie van het fonds
  - Contracten (incidentrespons, schade-expertise)
  - Toelatingsvoorwaarden
  - Reglementen
  - Etcetera
- Advies: lopende verzekeringen/retainers nog aanhouden
  - Medio 2025 meer duidelijkheid over tijdpad

mbo digitaal

Samenwerken met cloudleveranciers

- Vrijwel alle systemen binnen het mbo draaien bij externe leveranciers
- De school is/blijft verantwoordelijk: maak goede afspraken
- Goede overeenkomsten (SLA’s, verwerkersovereenkomsten)
- Zie toe op de veiligheidswaarborgen van de leverancier
- Voor de meestgebruikte systemen proberen we dat centraal te doen
- Bijvoorbeeld door de uitvoering van sectorale DPIA’s
  - SURF Vendor Compliance dienst
    bijdrage voor de mbo-scholen wordt tot 2027 vanuit de subsidie betaald
  - DPIA’s in opdracht van het programma Cyberveiligheid

mbo digitaal

Samenwerken met cloudleveranciers

DPIA’s die vanuit het programma Cyberveiligheid zijn/worden uitgevoerd:

Testjeleefstijl	Verwachte oplevering in december 2024
Digibib - Consortium	Verwachte oplevering in december 2024
Intergrip	Verwachte oplevering in december 2024
VOROC	Afgerond
Praktijkleren	Afgerond
Remindo (Paragin)	Afgerond
TOA	Afgerond
ESS	Afgerond
PortalPlus	Afgerond
Eduarte	Afgerond
Onstage	Afgerond
Ontrac	Afgerond

Zie ook het interview met Topicus Eduarte hierover

mbo digitaal

Hoe staat het met de volwassenheid op het gebied van IB?

- SURFaudit toetsingskader (NBA Volwassenheidsmodel IB)
  - mbo, hbo en universiteiten
- Jaarlijkse SURFaudit benchmark op het gebied van IB

Benchmark IB 2024	MBO	HBO	WO
Type audit	zelf-evaluatie	(grotendeels) externe audit	externe audit
Gemiddelde score	**2,3**	**2,1**	**2,5**

- Ook het mbo gaat nu over op externe security audits
- De eerste 6 audits zijn met Deloitte geëvalueerd

mbo digitaal

Resultaten externe security-audits (n=6)

Governance	MBO Gemiddelde
G0.01 Strategie	2,5
GO.02 Beleid	2,5
GO.03 Planning/roadmap	2,3
GO.04 Architectuur	1,7
GO.05 Onafhankelijke toetsing	1,8

Organisatie	MBO Gemiddelde
OR.01 Eigenaarschap, rollen, verantwoording en verantwoordelijkheid	2,5
OR.02 Functiescheiding	1,8

Risicobeheer	MBO Gemiddelde
RM.01 Informatie risicomanagement raamwerk	2
RM.02 Risicobeoordeling	2
RM.03 Plan voor behandeling en beperking van risico's	2

Personeelsbeheer	MBO Gemiddelde
HR.01 Werving	2,5
HR.02 Certificatie, training en scholing	2
HR.03 Afhankelijkheid van individuen	1,8
HR.04 Verandering of beëindiging van functie	1,8
HR.05 Kennisdeling	1,8
HR.06 Veiligheidsbewustzijn	3,3

Configuratiebeheer	MBO Gemiddelde
CO.01 Identificatie en onderhoud van config items	2,2
CO.02 Configuratie repository en baseline	2,5

Incident-/Probleembeheer	MBO Gemiddelde
IM.01 Incident management	2,2
IM.02 Incident escalatie	2,2
IM.03 Incident respons op (cyber) security incidenten	2,3
IM.04 Probleemmanagement	1,8

Wijzigingsbeheer	MBO Gemiddelde
CH.01 Normen en procedures voor aanpassingen	1,8
CH.02 Impact assessment, prioriteren en autoriseren	2
CH.03 Noodaanpassingen	1,8
CH.04 Testomgeving	1,7
CH.05 Testen van aanpassingen	2
CH.06 Promotie naar productie	1,8

Systeemontwikkeling	MBO Gemiddelde
SD.01 Methodologie voor veilige softwareontwikkeling en –implementatie	1,8
SD.02 Toegang tot de productieomgeving door ontwikkelaars	1,5
SD.03 Data conversie en/of migratie	2,2

mbo digitaal

Resultaten externe security-audits (n=6)

Gegevensbeheer	MBO Gemiddelde
DM.01 Data (en systeem) eigenaarschap	1,7
DM.02 Classificatie	1,8
DM.03 Beveiligingseisen voor gegevensbeheer	1,8
DM.04 Inrichting van opslag en retentie	2,2
DM.05 Uitwisseling van (gevoelige) gegevens	1,8
DM.06 Verwijdering van data	2

Identiteits- en Toegangsbeheer	MBO Gemiddelde
ID.01 Toegangsrechten	2
ID.02 Administratie van toegangsrechten	1,7
ID.03 Super users	1,5
ID.04 Noodtoegang	1,2
ID.05 Periodieke beoordeling van toegangsrechten	1,5

Beveiligingsbeheer	MBO Gemiddelde
SM.01 Security baselines	1,5
SM.02 Authenticatiemechanismes	2
SM.03 Mobiele apparatuur en telewerken	1,3
SM.04 Logging	2,3
SM.05 Testen, inspectie en toezicht op beveiliging	2,2
SM.06 Patchbeheer	2,3
SM.07 Beheer van bedreigingen & kwetsbaarheden	2,3
SM.08 Beschikbaarheid en bescherming van infra	1,8
SM.09 Onderhoud van de infrastructuur	2
SM.10 Beheer van cryptografische sleutels	1,3
SM.11 Netwerk beveiliging	1,7
SM.12 Beheersing van malware-aanvallen	1,8
SM.13 Bescherming van beveiligingstechnologie	2

Fysieke beveiliging	MBO Gemiddelde
PH.01 Fysieke beveiligingsmaatregelen	2,3
PH.02 Beheer van fysieke toegangsrechten	2,2

IT-operatie	MBO Gemiddelde
OP.01 Taakverwerking	1,4
OP.02 Procedures voor back-up en herstel	1,8
OP.03 Capaciteits- en prestatiebeheer	1,7

Bedrijfscontinuiteitsbeheer	MBO Gemiddelde
BC.01 Bedrijfscontinuïteitsplanning	1,7
BC.02 Testen van disaster recovery	1,5
BC.03 Offsite back-upopslag	1,7
BC.04 Gegevensreplicatie	1,8
BC.05 Crisisbeheer	2,2

Ketenbeheer	MBO Gemiddelde
SC.01 Service level overeenkomst	2,3
SC.02 Service level beheer	1,8
SC.03 Risicobeheer	1,7
SC.04 Supply chain management	1,8

mbo digitaal

Aandachtspunten vanuit de security audits

- Domein ***Gegevensbeheer***: besproken tijdens vorige gebruikersdag
  - Eigenaarschap
  - Classificatie
  - Bewaartermijnen / opschonen
  - ➢ nieuw: opzetten activiteiten rond ‘Digital Cleanup Day’

Verdieping voor vandaag: het domein ***Identiteits- en toegangsbeheer***
(Identity & Access Management, IAM)

➢ wie ben je (identificatie)

➢ wat mag je (autorisatie)

mbo digitaal

IAM: waarom is dat zo belangrijk

- De uitgangspunten van de AVG: doelbinding
  - Toegang tot persoonsgegevens die je echt nodig hebt voor je werk, bijvoorbeeld:
    - zorggegevens: alleen voor het zorgteam
    - begeleidingsgegevens: alleen voor de SLB-er
    - aan-/afwezigheidsgegevens: alleen voor de groepen aan wie de docent lesgeeft
- Informatiebeveiliging
  - Beperk de toegang tot informatie om het risico op een security-incident te verkleinen

mbo digitaal

IAM: wat zegt ons toetsingskader?

NBA - ID01

*De organisatie heeft toegangsgroepen (of **rollen**) gedefinieerd op basis van vastgestelde **bedrijfsregels**, waaronder functiescheiding, in een **SOLL-autorisatiematrix**. Er zijn **procedures** die tijdige initiatie en update in de SOLL-autorisatiematrices voor alle toepassingen regelen. Het **management** keurt wijzigingen in vastgestelde rechten voor toegangsgroepen (of rollen) goed. Alle gebruikers activiteiten zijn **traceerbaar** tot op het individu (bijv. gebaseerd op een combinatie van gebruikersnaam en wachtwoord of token of biometrische informatie).*

mbo digitaal

IAM: wat zegt ons toetsingskader?

NBA - ID02

Toegangsrechten voor werknemers worden toegewezen in ***overeenstemming met toegewezen taakverantwoordelijkheden*** *(bijvoorbeeld via op rollen gebaseerde toegang).* ***Beheerprocedures*** *zijn beschikbaar om activiteiten vast te stellen voor het* ***aanvragen***, ***uitgeven*** *of* ***sluiten*** *van een account en de bijbehorende toegangsrechten voor gebruikers. De procedure omvat tevens de methode die door het* ***senior management*** *wordt gebruikt om deze activiteiten op de juiste wijze te* ***autoriseren****. Toegang wordt verschaft op basis van het* ***need-to-know/need-to-have principe****.*

mbo digitaal

IAM: wat zegt ons toetsingskader?

NBA - ID05

*Het **management beoordeelt** periodiek de gebruikerstoegang die geïmplementeerd is voor de relevante applicaties (IST-situatie) om de **juistheid** van geïmplementeerde accounts en rollen (de toegangsrechten) te bevestigen, en valideert dat toegangsrechten **passend zijn** voor toegewezen taken, zoals bepaald door de toegangsregels (SOLL-situatie). Elke onjuiste toegang die tijdens het beoordelingsproces wordt opgemerkt, wordt direct ingetrokken. Deze controle houdt in dat **SOLL- en IST-matrices worden vergeleken** door het verantwoordelijke management.*

mbo digitaal

IAM: waarom is dat zo ingewikkeld?

- Doe mee en beantwoord deze vragen in de Menti:

- Daarna neemt Bas van Loenen het stokje over met een presentatie over de aanpak van IAM bij Albeda
- Dank voor jullie aandacht!

Martijn Bijleveld | m.bijleveld@mbodigitaal.nl
https://mbodigitaal.nl/programma-cyberveiligheid-mbo

PROGRAMMA
Cyberveiligheid