mbo digitaal

Inrichten logische toegangsbeveiliging in het MBO

Samen slim inrichten

Logische toegangsbeveiliging heeft extra aandacht nodig. We delen initiatieven uit het programma cyberveiligheid (standaard beleid, best practices en templates).

Henry Meutstege

5 maart 2026

V1.0

mbo digitaal

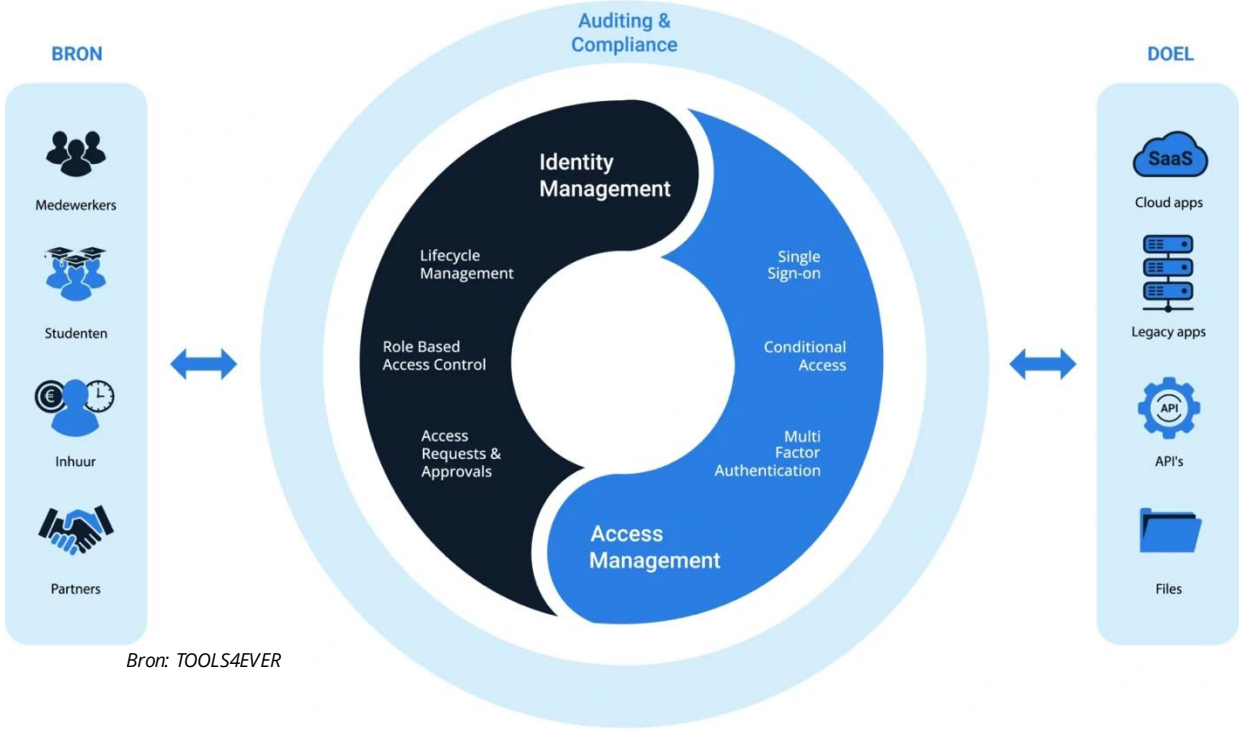
Agenda

- Waarom is Logische toegangsbeveiliging belangrijk?
- De neuzen dezelfde kant op
- Bouwstenen
- Techniek & beveiliging
- Toetsingskader
- Templates
- Discussie
- IAM-werkgroep

mbo digitaal

Waarom is Logische Toegangsbeveiliging belangrijk?

- Logische toegangsbeveiliging of ook wel Identity en Acces Management (IAM)
- Alle deuren en ramen zijn op slot, echter je hebt geen idee wie de sleutels heeft… en welke sleutels er zijn
- IAM is een belangrijk domein om IB & Privacy aantoonbaar op orde te houden.
- Audits laten lage volwassenheid zien op IAM.
- IAM koppelt toegang aan betrouwbare brondata en rollen; minder handwerk, minder fouten en betere verantwoording.
- Voor deelname aan de Cyberweerbaarheidspool is compliance vereist op het IAM-domein.



Bron: TOOLS4EVER

De neuzen dezelfde kant op....
(Definities)

Logisch Toegangsbeheer (Identity and Access Management): processen, technologieën en afspraken die bepalen wie toegang heeft tot wat, wanneer en onder welke voorwaarden.

Kernbegrippen:

- Identificatie: digitale identiteit (attributen)
- Authenticatie
- Autorisatie
- Provisioning & deprovisioning
- Levenscyclusbeheer (instroom, doorstroom, uitstroom)

mbo digitaal

Bouwstenen van IAM

IAM werkt alleen als de basis klopt: betrouwbare brondata en een helder rechtenmodel.

Bronsystemen (fundament)
- HRM (medewerkers), SIS (studenten), registraties voor externen

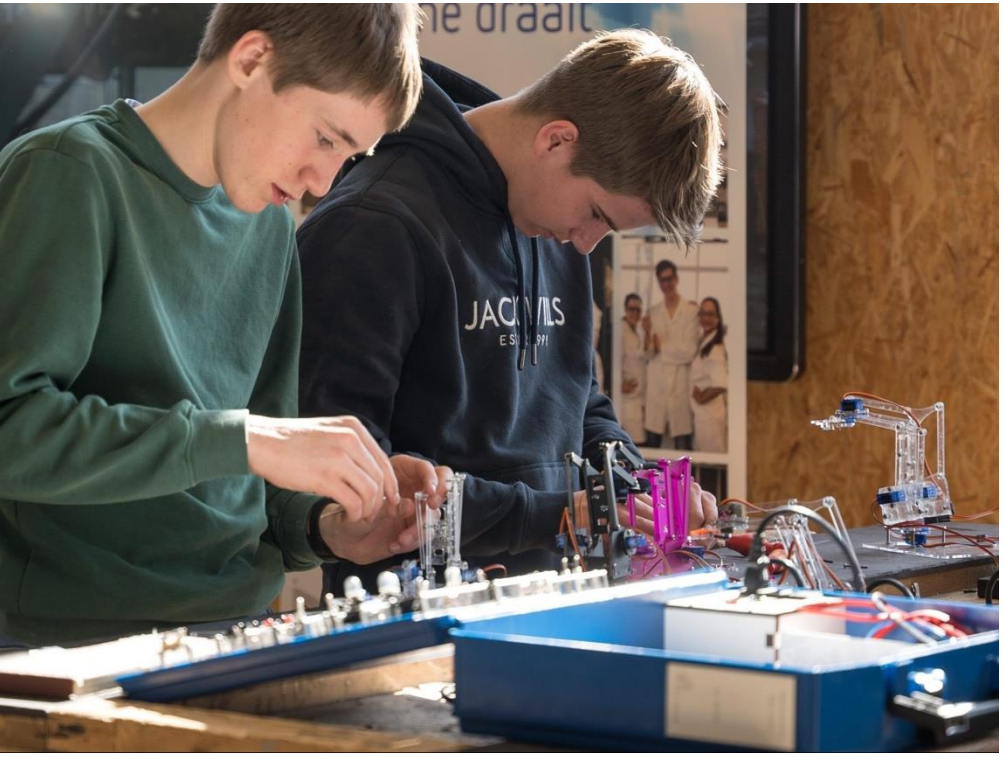
Datakwaliteit & eigenaarschap
- Actuele en volledige gegevens
- Eigenaarschap bij HR / onderwijsadministratie

Attributen & autorisatiematrix
- IAM beslist op attributen (rol, afdeling, locatie, start/einddatum)
- Autorisatiematrix koppelt attributen aan rechten

Betrouwbare brondata → juiste attributen → vastgesteld rechtenmodel → gecontroleerde toegang

mbo digitaal

Techniek & beveiliging



Organisatie bepaalt de regels

- Bronsystemen (HRM/SIS) leveren rollen, functies, start/einddatums.
- Autorisatiematrix bepaalt: *welke rol krijgt welke rechten?*

IAM voert dit technisch uit

- Identity store (AD/ Entra ID): centraal overzicht van alle identiteiten.
- Provisioning: automatische toekenning en intrekking van rechten.
- Authenticatie: wachtwoord + MFA → bepaalt *wie* inlogt.

Beveiligingslagen versterken elkaar

- MFA + SSO
- PAM/JIT voor beheeraccounts
- Break-glass/noodprocedures
- Logging + periodieke reviews (IST ↔ SOLL)

De organisatie bepaalt *wat* er moet gebeuren, IAM-techniek voert het automatisch en gecontroleerd uit.

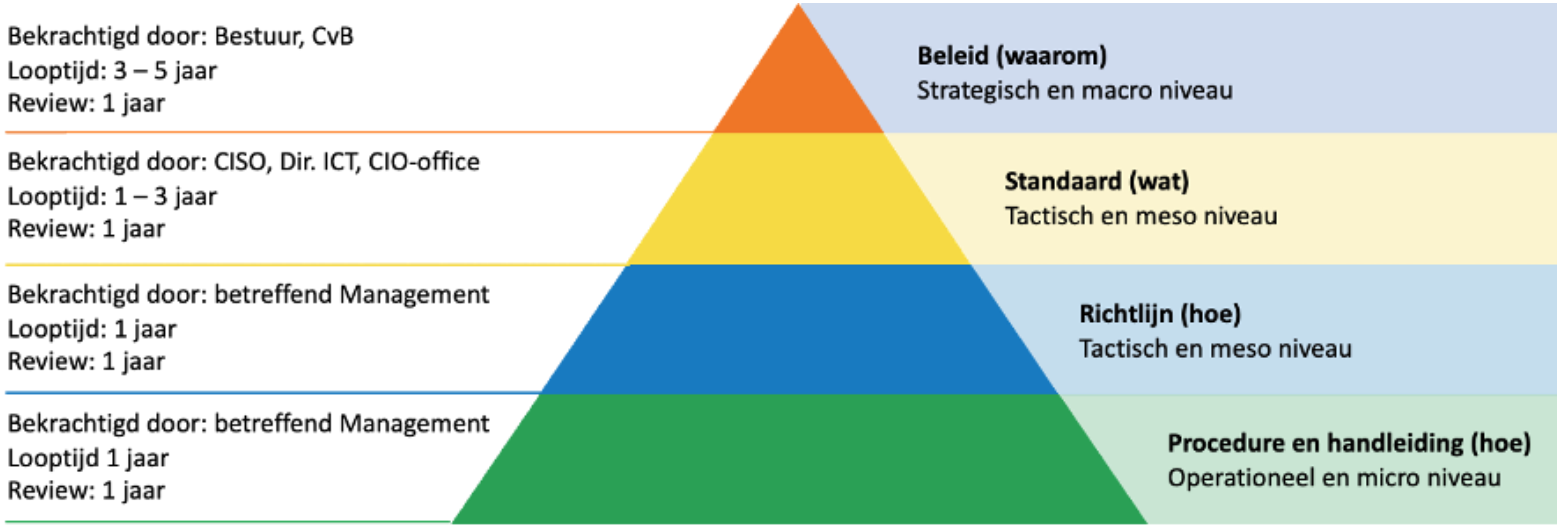
mbo digitaal

SURFaudit toetsingskader IB

Statemen	Onderwerp	Waar het om gaat
OR.02	Functiescheiding	Taken worden gescheiden zodat één persoon geen kritieke processen kan beïnvloeden.
HR.04	Verandering of beëindiging van functie	Bij functiewijziging of vertrek worden verantwoordelijkheden opnieuw toegewezen en toegangsrechten direct verwijderd om continuïteit en veiligheid te borgen.
ID.01	Toegangsrechten	Rollen en rechten zijn vastgelegd in een autorisatie-matrix (SOLL) en herleidbaar per gebruiker.
ID.02	Administratie van toegangsrechten	Toegang wordt toegekend, gewijzigd en ingetrokken via formele, controleerbare procedures.
ID.03	Super-user toegang	Super-user rechten zijn beperkt, goedgekeurd en worden gemonitord.
ID.04	Noodtoegang	Noodprocedures zijn gedocumenteerd, gelogd en geëvalueerd.
ID.05	Periodieke toetsing	SOLL- en IST-situatie worden vergeleken, afwijkingen worden hersteld.
SM.02	Authenticatiemechanismes	Unieke accounts, centraal beheerd. Authenticatie volgens beleid (incl. MFA). Functiescheiding in aanvragen en toekennen. Inactieve accounts worden tijdig verwijderd.

Templates: SURF & MBO Digitaal

- SURF-templates
  - Standaard identiteits- en toegangsbeheer
  - Richtlijn toekennen en intrekken autorisaties
  - Richtlijn autorisatiebeheer en controle
  - Template Autorisatiematrix
  - Handreiking Richtlijn Wachtwoorden
  - Handreiking Wachtwoorden kluis



- Programma Cyberveiligheid: pragmatisch beleidsdocument (netwerk IB&P, afgeleid van SURF templates)
- Voor Cyberweerbaarheidspool compliance: focus op de kroonjuwelen

Discussie (1/3)

Stelling:

De data eigenaar bepaald wie toegang krijgt tot een applicatie

Eens of oneens?

Discussie (2/3)

Stelling:

Elke beheerder heeft super user rechten nodig om zijn werk goed te kunnen doen

Eens of oneens?

Discussie (3/3)

Stelling:

Een autorisatiematrix bestaat uit een overzicht van rollen, de rechten die bij de rol horen en een overzicht van gebruikers die deze rol hebben…

Eens of oneens?

mbo digitaal

IAM-werkgroep

Doel:

- Delen best practices
- Concrete templates en procedures opleveren
- Voorbeeld autorisatie matrix voor Eduarte!
- Referentie rollen uit de MORA gebruiken voor autorisatie matrix