

Event privacy en informatiebeveiliging in het onderwijs

R. (Ruud) Buurma, L. (Lodewijk) Benjaminse en H.S. (Helen) van Reenen
mei 2021

OPENBAAR

-
1. Introductie
 2. Oorzaken en risico's
 3. Oplossingsrichtingen
 4. Samenvatting



Introductie Voorstellen



L. (Lodewijk) Benjaminse

directeur

lodewijk.benjaminse@hodari.nl

071-2032385

Lodewijk heeft meer dan 15 jaar ervaring als adviseur en auditor binnen informatiebeveiliging en privacy onder andere bij onderwijsinstellingen.



H.S. (Helen) van Reenen

adviseur

helen.van.reenen@hodari.nl

06-15052672

Helen heeft ruime ervaring op het gebied van implementaties van IT oplossingen voor gebruikers. Haar focus is verschoven van techniek naar mens en motivatie.



R. (Ruud) Buurma

adviseur

ruud.buurma@hodari.nl

06-26396625

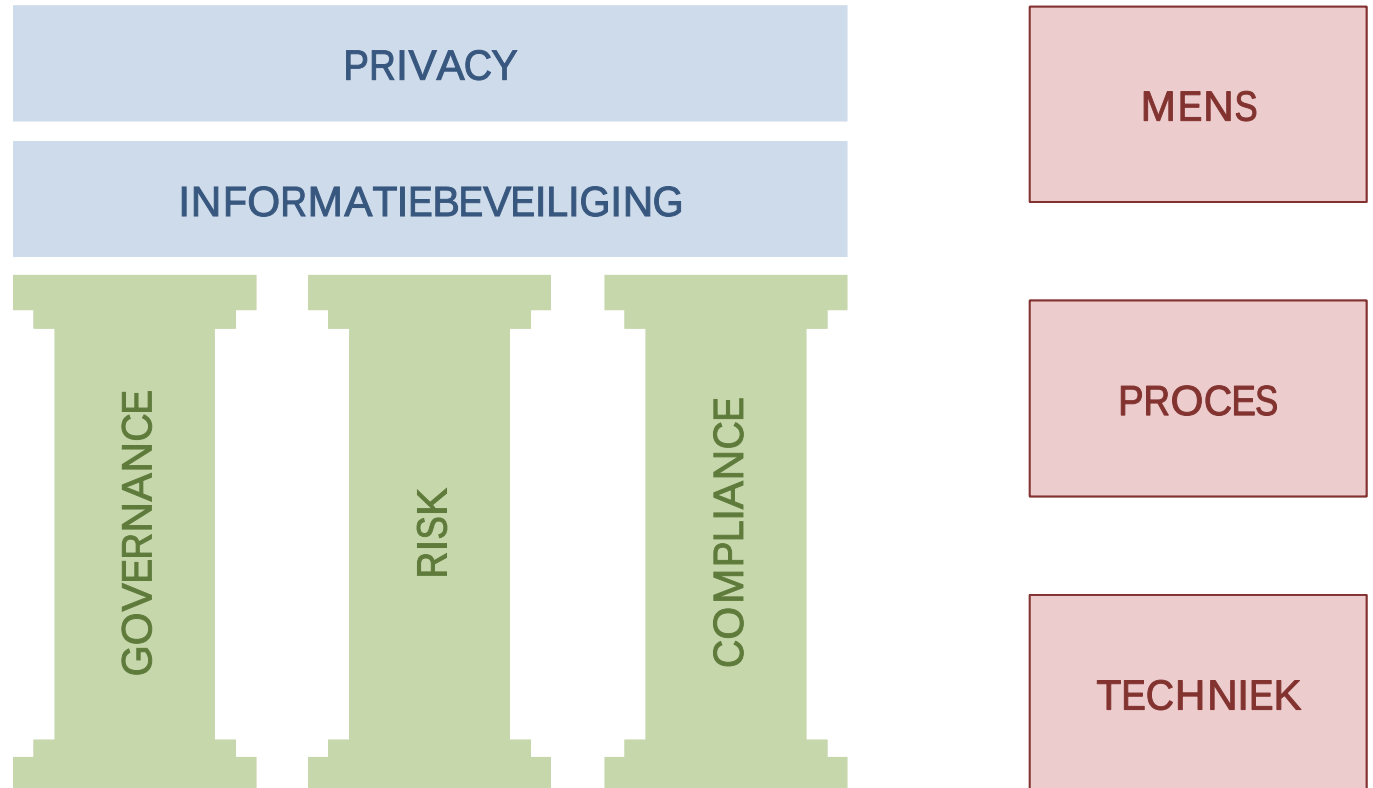
Ruud heeft ruime ervaring op het gebied van informatiebeveiliging en privacy. Hij heeft projecten geleid bij onder andere een private onderwijsorganisatie.

Introductie

Missie en visie

missie: HODARI draagt bij aan een betere informatiebeveiliging en privacy met een veiligere samenleving als doel

visie: HODARI helpt organisaties aantoonbaar en blijvend grip te krijgen op informatiebeveiliging en privacy door vraagstukken op het gebied van governance, risk en compliance op te lossen



Introductie

Uit het nieuws

- Aantal DDoS-aanvallen tegen online lesomgevingen groeide in het voorjaar van 2020 exponentieel in vergelijking met het voorgaande jaar. (Digital Education report van Kaspersky, september 2020)
- Tevens is een toenemend aantal verschillende bedreigingen geconstateerd, die zijn verspreid onder het mom van populaire online leerplatforms / videogesprekstoepassingen. (Digital Education report van Kaspersky, september 2020)
- *“Aandacht nodig voor weerbaarheid tegen cyberaanvallen”*
(Onderwijsinspectie, maart 2021)



Introductie

Uit het nieuws

- *“Clop-ransomware infecteert systemen Universiteit Maastricht”*
(security.nl, december 2019)
- Privégegevens van alumni, donateurs en relaties van de Universiteit Utrecht en TU Delft in handen van hackers gekomen vanaf een back-up bij een leverancier. (Universiteit Utrecht en TU Delft, mei 2020)
- *“UvA en HvA zijn het doelwit geweest van een zware cyberaanval.”*
(UvA en HvA, maart 2021)
- *“Onbekenden hebben gegevens buitgemaakt van tienduizenden studenten en medewerkers van Hogeschool Inholland. De data worden te koop aangeboden op een hackersforum.”*(Rijnmond, maart 2021)



-
1. Introductie
 2. Oorzaken en risico's
 3. Oplossingsrichtingen
 4. Samenvatting



Oorzaken en risico's

Risicoanalyse

- **Stap 1:** Inventarisatie van belangrijkste assets / middelen
- **Stap 2:** Identificeren van risico's
- **Stap 3:** Bepalen van prioriteit van risico's
- **Stap 4:** Risico mitigatie strategieën:
 - overdragen;
 - vermijden;
 - accepteren;
 - reduceren.
- **Stap 5:** Bepalen van maatregelen

Risico: kans x impact

Voorbeeld van risico's binnen het onderwijs zijn:

- hack;
- datalek;
- onzorgvuldig gebruik wachtwoord.

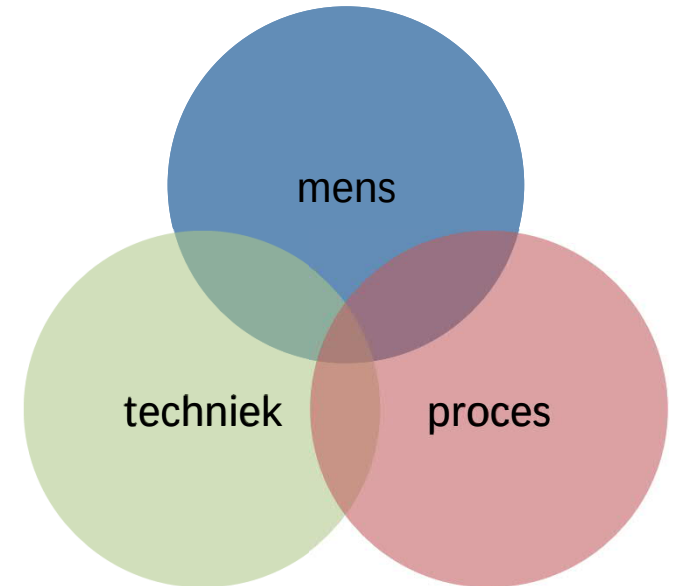


Oorzaken en risico's

Oorzaken

Mens:

- gewenning en cultuur;
- gebruik van niet geregleerde applicaties, software, ...;
- onbekendheid met de risico's;
- onbekendheid met wet- en regelgeving.

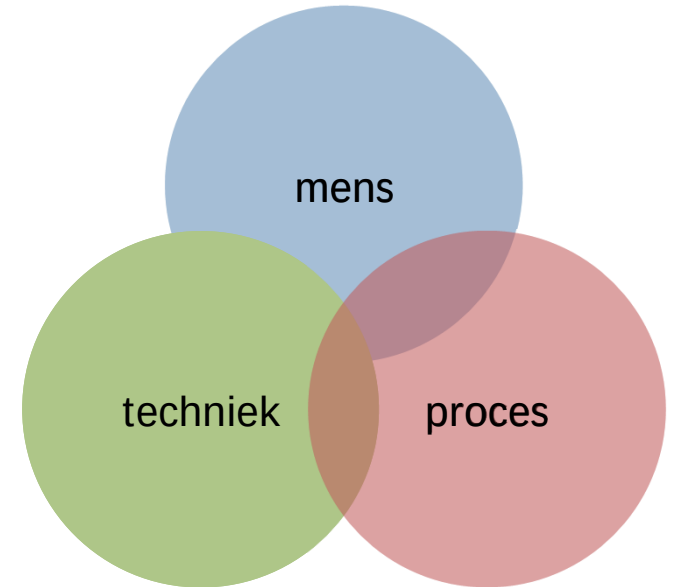


Oorzaken en risico's

Oorzaken

Techniek:

- gebruik van onveilige verbindingen;
- gebruik van onveilige wachtwoorden;
- onveilige opslag en back-up;
- ruime autorisaties en toegang tot gevoelige gegevens.

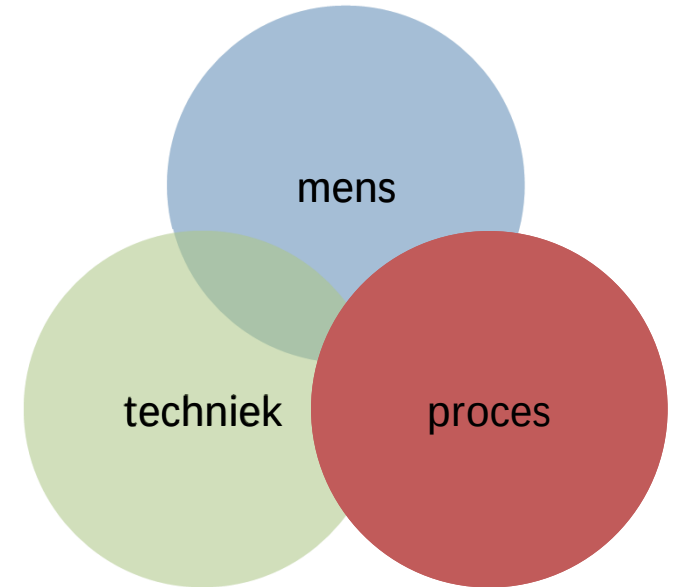


Oorzaken en risico's

Oorzaken

Proces:

- geen formeel beleid en procedures;
- informatiebeveiliging en privacy zijn in het onderwijs nog in ontwikkeling;
- inrichten van complexe structuren ten aanzien van identity and access management;
- beperkte capaciteit voor informatiebeveiliging en privacy;
- het onderwijs committeert zich nog in beperkte mate aan standaarden.



-
1. Introductie
 2. Oorzaken en risico's
 3. Oplossingsrichtingen
 4. Samenvatting



Oplossingsrichtingen

Veel adviezen en handreikingen beschikbaar

- Autoriteit Persoonsgegevens;
- SURF;
- Kennisnet;
- Inspectie van het onderwijs;
- ISO 21001 Management systems for educational organisations;
- ISO 9001 Kwaliteitsmanagement;
- ISO 27001 en 27002 Informatiebeveiliging;
- Privacy covenant MBO-, HBO- en PO-raad.

Privacy en informatiebeveiliging:

- gefragmenteerd;
- behoudens AVG niet afgedwongen;
- samenhang ontbreekt;
- best practice ontbreekt;
- eigen wiel uitvinden.



Oplossingsrichtingen

Introductie

Uitgangspunten:

- elke onderwijsinstelling verwerkt op grote schaal persoonsgegevens;
- de verwerking van persoonsgegevens moet voldoen aan de wettelijke kaders;
- een onderwijsinstelling moet dat kunnen aantonen;
- transparantie en het afleggen van verantwoording aan betrokkenen;
- delen van inlogcodes, onbeveiligd e-mailen van gegevens over leerlingen en studenten aan de orde van de dag;
- meer mensen dan noodzakelijk hebben toegang tot gegevens van leerlingen;
- datalekken, cybercriminaliteit en andere beveiligingsincidenten komen steeds meer voor;
- accountants beoordelen, in het kader van het opstellen van de jaarrekening, de betrouwbaarheid en continuïteit van de ICT-systemen;
- boetes van de Autoriteit Persoonsgegevens vormen een risico wanneer privacy en informatiebeveiliging onvoldoende zijn geregeld.



Oplossingsrichtingen

Techniek

Preventie:

- bescherming tegen malware;
- redundante componenten;
- beveiligde inloggen, bijvoorbeeld door middel van multi factor authentication.

Detectie:

- respons op incidenten;
- back-up;
- logfiles;
- continuïteitsplan.



Oplossingsrichtingen

Proces

Beleid en verantwoordelijkheden:

- beleid bevat: uitgangspunten, maatregelen, procedures en afspraken;
- zeggenschap, toezicht, wie is verantwoordelijk, eigenaarschap;
- information security officer;
- functionaris voor privacy;
- champions.

Beleid uitwerken en implementeren van procedures zoals:

- omgaan met social media;
- gedragscode;
- hanteren beveiligingscamera's;
- melding incidenten (in bijzonder datalek);
- wachtwoordbeleid;
- veilige netwerkomgeving;
- bewaartermijnen;
- back-up;
- rechten van betrokkenen.



Oplossingsrichtingen

Proces

Monitoren en evalueren:

- verantwoordings- en informatieplicht, rapportages;
- assessments;
- bijsturen;
- integraal framework voor privacy en informatiebeveiliging.

Denk aan de PDCA-cyclus!

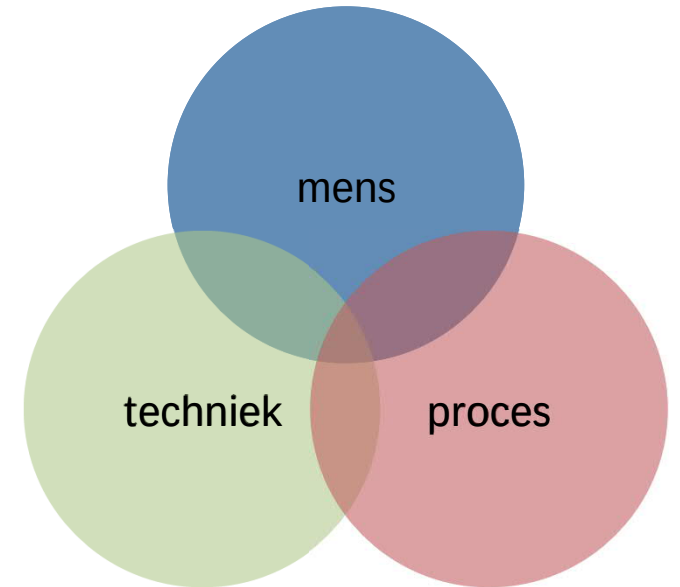


Oplossingsrichtingen

Mens

Het belangrijkste aspect om informatiebeveiliging en privacy te verbeteren is en blijft de mens:

- duidelijke tone at the top;
- eindgebruikers bewust maken van de risico's van cybercrime;
- creëer een vertrouwenscultuur waarbij betrokkenen veiligheidsrisico's signaleren en durven te melden.



Oplossingsrichting

Mens

Gedragsbeïnvloeding is het moeilijkste deel:

- in cybersecurity gebruikt men het AMC framework;
- drie componenten tot aansporing;
- voor zowel staf, docenten en studenten;
- biedt een helder en eenvoudig model op basis van gedragspsychologie uit *“The Influence of Knowledge and Attitude on Intention to Adopt Cybersecure Behaviour”*. (L.C. de Kok, D. Oosting en M. Spruit, 2020).

AMC framework: **gedrag** is een combinatie van:

$\text{awareness} \times \text{motivation} \times \text{capability}$



Oplossingsrichting Mens

Drie componenten:

- **awareness:** kennis, noodzaak, het nut en de voordelen;
- **motivation:** persoonlijke overtuiging;
- **capability:** je hebt toegang tot middelen.

AMC framework: **gedragsverandering** is
een combinatie van:

leren × motiveren × faciliteren



Oplossingsrichting

Mens: awareness

Awareness ten aanzien van informatiebeveiliging en privacy gaat ook om waarden:

- Het **waarom** en het **doel** van een cultuur van informatiebeveiliging en privacy.
- De **bedreiging** die het gevolg is van gebrek aan bescherming op individueel niveau tegelijk met het bieden van een **mogelijkheid om actie te ondernemen**.
- De **regels en processen** die gevolgd moeten worden, met de handhaving die u daarbij wil toepassen. Duidelijkheid over de sancties en de **beloning**, op individueel niveau en op groepsniveau.
- Het belang van **samenwerking** en **gelijkwaardigheid**. Eventuele uitzonderingen zijn vooraf bekend.
- De mogelijkheid om, als de regels onvoorzien te beperkend zijn, in gesprek te gaan over **verbeteringen en aanpassingen**.

Waarden:

- veiligheid en verbinding;
- zelfredzaamheid;
- duidelijke regels en naleving;
- beloning en succes;
- gelijkwaardigheid;
- vrijheid;
- groter doel.

Trainingen dragen bij in het vergroten van awareness.



Oplossingsrichting

Mens: motivation

Het menselijke aspect: persoonlijke aandacht:

- motivation wordt meer bepaald door gevoelens;
- gedrag wordt bepaald door anderen in de directe omgeving;
- herhaaldelijk ervaringsgericht leren vergroot de motivatie;
- met behulp van spellen worden de gesprekken gemakkelijker.

Voorbeelden van interactieve werkvormen zijn te vinden op kennisnet:

“Aanpak informatiebeveiliging en privacy in het onderwijs”, zie

<https://aanpakibp.kennisnet.nl/bewustwording>.

De menselijke maat:

- De dreiging komt van een persoon, de hacker, die gelegenheden zoekt om zichzelf te verrijken en zich daarbij niets van jouw persoonlijk leed aantrekt.
- Het aanspreken en reageren op persoonlijke morele waarden ten aanzien van veiligheid vergroot de motivation.



Oplossingsrichting

Mens: capability

Goede capability versterkt gewenst gedrag:

- de mogelijkheid om het gevraagde beleid uit te voeren;
- laagdrempelig, vindbaar, makkelijk uitvoerbaar;
- technisch in orde, goede terugkoppeling;
- expert aanwezig;
- eenvoudige instructies en simpele handelingen;
- gemakkelijk te onthouden.

PDCA-cyclus:

- herhaal de regels, het waarom en de impact;
- leef dit binnen de top en op alle lagen;
- maak een gewoonte van goed gedrag rondom informatiebeveiliging en privacy;
- beloning is onderdeel van de cultuurverandering;
- op de langere termijn ontstaat een nieuwe vertrouwens cultuur;
- blijf meten en terugkoppelen.



Oplossingsrichting Mens

Door te meten weet je welke component ontbreekt:

- **plan:** inventariseer hoe het nu is met de awareness, motivation en capability;
- **do:** communiceer over de opzet en de middelen;
- **check:** meet het effect, en analyseer;
- **act:** verbeter door middel van leren, motiveren of faciliteren.

AMC framework:

- maak gedrag een onderdeel in de PDCA-aanpak;
- alle drie de componenten moeten voldoende aanwezig zijn;
- ontbreekt er één, dan vindt er geen gedragsverandering plaats.



-
1. Introductie
 2. Oorzaken en risico's
 3. Oplossingsrichtingen
 4. Samenvatting



Samenvatting

Inrichten van privacy en informatiebeveiliging

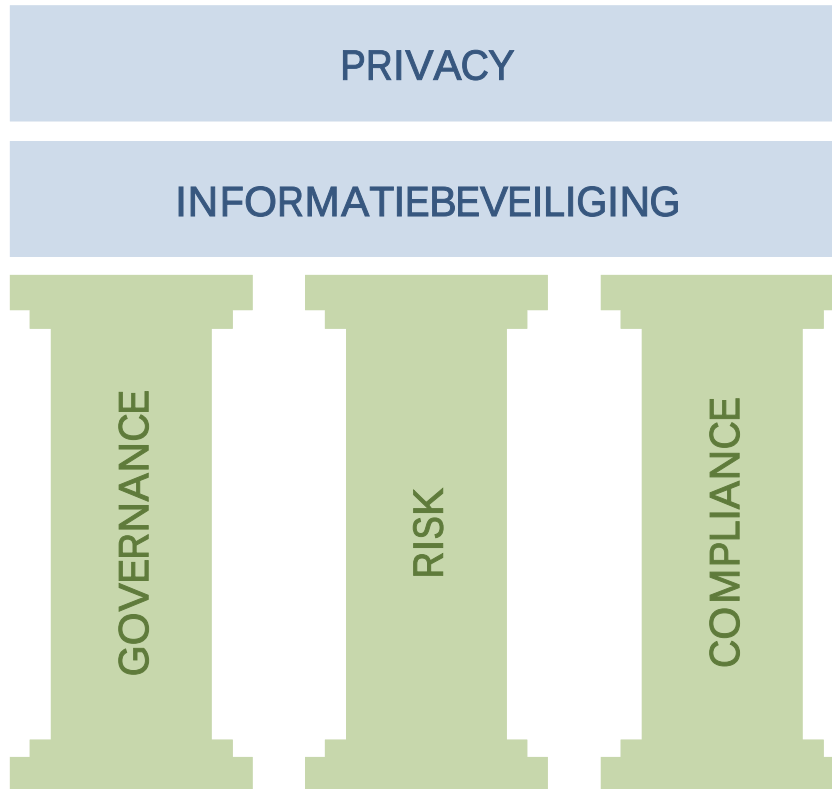
Inrichten van privacy en informatiebeveiliging op basis van scan, assessment en risicoanalyse en vaststellen en definiëren van maatregelen en deze te implementeren, zoals:

- het opstellen van een jaar- of meerjarenplan;
- het ontwikkelen van privacybeleid en informatiebeveiligingsbeleid;
- implementatie van voor privacy en informatiebeveiliging relevante procedures;
- implementatie van managementsystemen en beveiligingsmaatregelen;
- ondersteuning/coaching van verantwoordelijken voor privacy, informatiebeveiliging of kwaliteit;
- geven van bewustwordingstrainingen aan betrokkenen;
- invulling van de rol van Functionaris voor Gegevensbescherming, privacy officer of information security officer in een onderwijsinstelling.



Samenvatting

Afronding



HODARI draagt bij aan betere informatiebeveiliging en privacy met een veiligere samenleving als doel. HODARI helpt organisaties aantoonbaar en blijvend grip te krijgen op informatiebeveiliging en privacy door vraagstukken op het gebied van governance, risk en compliance op te lossen.

Wij bieden kwalitatief hoogwaardige oplossingen waarbij de meest complexe vraagstukken tot in detail zijn opgelost. Wij hebben ruime ervaring opgedaan binnen verschillende sectoren, zoals de financiële sector, onderwijs, energiesector, retail, (rijks)overheid, advocatuur en IT-dienstverleners. Regelmatig handelen wij binnen projecten naar aanleiding van fusies en overnames, reorganisaties, bevindingen van

HODARI B.V.

071-2032385

hodari.nl

L. (Lodewijk) Benjaminse

lodewijk.benjaminse@hodari.nl

06-53736105