Office 365 en Informatieveiligheid

Microsoft® Office 365

Mark de Jong, Hogeschool Inholland
13 april 2018

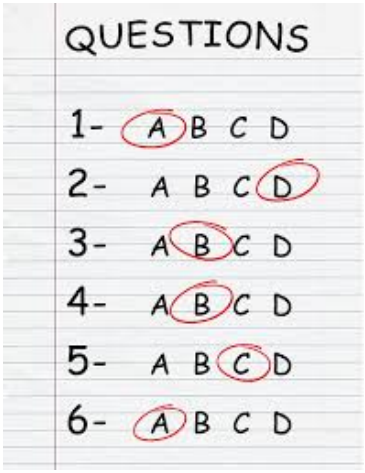
Office 365 en Informatieveiligheid

1. Strategie Inholland
2. Uitdaging Office 365 en OneDrive
3. Risicoanalyse
4. Keuzes
5. Discussie

Hoe bescherm je (of verbeter je) privacy en informatieveiligheid binnen Office 365?

Strategie Inholland

Welke belangrijke data heeft Inholland?



PERSOONSGEGEVENS

DAAR ZIJN WE ZUINIG OP

Palet aan maatregelen

- Proces
- Organisatie
- Fysiek
- ICT/ Techniek
- Gedrag
- Bewustzijn
- Cultuur
- Communicatie
- Juridisch

Wat wil Inholland?

1. Veilige omgeving bieden voor alle gebruikers
2. Ondersteunen en beschermen van missie, visie
3. Continuïteit van de instelling en het primaire proces waarborgen
4. Informatieveiligheid als competentie van de (toekomstige) professional
5. Voldoen aan wet- en regelgeving


Tevreden en succesvolle studenten
Duurzaam
Een omgeving waar je op een veilige manier fouten mag maken
Durf te leren
Creatief
Gezond
Stadsoverstijgend
hogeschool
Onderwijs en onderzoek voor de toekomst

Uitgangsprincipe Inholland

Data in de hoogste vertrouwelijkheidscategorie in specifieke applicaties

Risicoanalyse Office365 en Onedrive

De implementatie van OneDrive brengt twee risico's met zich mee, namelijk

1. **vertrouwelijkheid** van informatie wordt geschaad (persoonsgegevens, toetsen)

2. **integriteit** van informatie wordt geschaad

Inschatting: Beiden risico's lopen we ook in de huidige situatie (F/H-schijf, SharePoint), maar de kans dat het risico zich voordoet is groter.

Oorzaken uitkomen risico (I)

- Onbekwaamheid met het werken in de nieuwe omgeving;
- Onduidelijkheid over de relatie tussen schijven (F, H) en OneDrive bij de gebruiker;
- Medewerker denkt dat wat organisatie aanbiedt, standaard op de juiste manier afgeschermd is;
- Informatie komt in een map terecht met te veel (gedeelde) rechten;

Oorzaken uitkomen risico (II)

- Medewerker weet niet op welke omgeving hij/ zij werkt (privé/ organisatie);
- Medewerker stuurt link door naar document, waardoor het document voor iedereen binnen de organisatie zichtbaar is;
- Medewerker werkt op eigen, onbeveiligde privé-omgeving en device en synchroniseert data, waardoor data buiten de Inholland-omgeving komt.

Gevolg uitkomen risico

- Schending wetgeving
- Boetes
- Reputatieschade
- Onveilig gevoel, verwarring en onvrede bij gebruikers

Uitlekken persoonsgevoelige data (datalek)
Uitlekken van gevoelige informatie (bijvoorbeeld toetsen)

Uitdaging: Office 365, rechten betrokkene

AVG / GDPR

- Toestemmingsvereiste: aantoonbaar en expliciet
- Recht op inzage (geen recht op inzage in documenten (WOB))
- Recht om vergeten te worden
- Recht op rectificatie
- Recht op dataportabiliteit
- Recht om bezwaar te maken tegen profiling

Inschatten huidige risiconiveau Office 365

We hebben de kans dat het risico zich voordoet en de mogelijke impact als volgt ingeschat:

Kans: **Hoog**
Impact: **Midden - Hoog**

Verwachting:
het risico in de loop van de tijd wordt kleiner, omdat medewerkers bekend raken aan de nieuwe omgeving

Zijn er ervaringen met richtlijnen om persoonsgegevens niet in bestanden te bewaren? (excel, word, ..)

Implementatie van maatregelen

- Proces
- Organisatie
- Fysiek
- ICT/ Techniek
- Gedrag
- Bewustzijn
- Cultuur
- Communicatie
- Juridisch

Welke maatregelen heeft uw instelling ingezet?

Maatregelen: proces / organisatie

- Functioneel beheer voor toekennen groepen/sites

- Autorisatiebeleid
  - Minimaliseren van toegang tot gegevens

- Gecontroleerde uitgifte lidmaatschap van groepen
  - Formele groepen (uit bronnen)
  - Semi-formele groepen (gedelegeerd beheer)

Maatregelen: bewustzijn

- Training gebruikers
  - Specifiek voor Office365
  - Meenemen in andere trainingen rond privacy, informatieveiligheid, veiligheid
- Bij uitgifte device
- Overeenkomst met regels rond gebruik Inholland device, Office 365 en OneDrive;

Maatregelen: techniek

- Sync toestaan op *domain joined devices* (in beheer van Inholland), maar voor andere situaties uitzetten;
- Uitzetten extern delen SharePoint-sites (tijdelijke maatregel, later tijdstip herzien en mogelijk gefaseerd aanzetten. Azure Information Protection / IRM voor beveiliging op documentniveau.)
- Delen via Groups als beginpunt uitzetten, en dan gecontroleerd openzetten (bijvoorbeeld via functioneel beheer)
- Default sharinglinks instellen op ‘direct – only people who already have permission’
- Inzet SURFsecureID voor 2FA bij verwerking data met classificatie Hoog

Implementatie bij andere scholen

- Welke keuzes maken andere instellingen?
- Welke kansen biedt Office365?
- Hoe garandeert de instelling de veiligheid van privacygevoelige data?
- In hoeverre laat de instelling de gebruikers vrij?
- Maakt de organisatie onderscheid tussen studenten en medewerkers?
- Heeft iemand al incidenten gehad?

Contact

Mark de Jong, Enterprise Architect
IVT Hogeschool Inholland
mark.dejong@inholland.nl
06 2295 7086


inholland
hogeschool