Informatiebeveiliging

ORB

Qixium staat voor betrouwbare koppelingen,
goede en duidelijke ondersteuning
bij de uitvoer en voor juiste Informering!

Informatiebeveiliging

Onderstaand zijn de aspecten met betrekking tot informatiebeveiliging van de ORB-toepassing op basis van het Qixium SaaS platform opgenomen. Scope4mation is ISO27001 gecertificeerd en heeft informatiebeveiliging hoog in het vaandel staan. Daarom zijn er zowel passende technische als organisatorische maatregelen genomen en geauditeerd binnen de kaders van de ISO27001 certificering.

Informatie over de beveiliging van het voor ORB benodigde account:

- Het Exchange/ O365 account dat door ORB benut wordt, heeft impersonation rechten nodig;
  - Hierdoor kan er een ruimte gereserveerd worden via ORB, vanuit de agenda van de organisator of namens de organisator
  - Het hiervoor benodigde account kan zo ingesteld worden, dat er niet mee ingelogd kan worden als gebruiker;
    - Dit wordt door de klant zelf op de mailbox van het account ingesteld.
    - Hiermee wordt het grootste risico van het account met deze rechten gemitigeerd, namelijk dat er niet mee ingelogd kan worden en er, in combinatie met onderstaande maatregelen, geen andere verwerking dan via de ORB-toepassing kan plaatsvinden.
  - Voor de communicatie met Exchange/ O365 kan Oauth2 gebruikt worden;
  - Het adres waarvandaan het Exchange/ O365 account gebruikt wordt kan door de klant zelf ge-white-list worden in de eigen klantomgeving;
    - Dit geldt voor de APP registratie of de EWS URL.
  - Het token dat benut wordt voor het account kan door de klant zelf in ORB Qixium worden ingevoerd;
    - Hiermee wordt voorkomen dat Scope4mation de inhoudelijke gegevens van het token kan benutten.
  - Alleen de ORB-toepassing zelf maakt hier gebruik van, mede omdat er met het account niet als user ingelogd kan worden.
    - Het token wordt gecodeerd (“encrypted”) opgeslagen binnen de Qixium ORB toepassing.

- Het TOPdesk account dat voor ORB benut wordt, kan binnen TOPdesk beperkte rechten krijgen waarmee alleen die functionaliteit beschikbaar is die nodig is om met ORB-reserveringen te kunnen maken
  - De verbinding met TOPdesk is voorzien van een certificaat en communicatie vindt plaats op basis van https;

Exchange / O635 Impersonation

Ter toelichting op Exchange/ O365 impersonation:

- Conform Microsoft zijn de aangegeven impersonation rechten nodig om door ORB-ruimtes namens een organisator te kunnen reserveren. Bovenstaande maatregelen zorgen ervoor dat niet met het ORB-account ingelogd kan worden, waarmee gebruik (lees misbruik) van het account voor andere doeleinden dan voor het gebruik voor de Qixium/ORB toepassing wordt voorkomen.

“Outlook” instelling

Aanvullende informatie over “Outlook” instelling:

- Binnen Exchange/ O365 kunnen instellingen gemaakt worden waarmee gegevens die door de ORB worden benut beperkt worden, zoals m.b.t. het onderwerp en de body van de mail.
    - Hierdoor worden deze gegevens, desgewenst, niet uitgewisseld met ORB
    - De body van de reservering/ meeting hoeft derhalve niet doorgegeven te worden aan ORB en kan dan derhalve ook niet doorgegeven worden naar TOPdesk
    - Deze instelling wordt binnen Exchange/ O365 gemaakt en kan derhalve alleen met een daarvoor bedoeld beheerdersaccount worden aangepast.
        - Het aanpassen van deze instelling staat geheel los van het ORB-account

Aanvullende informatie

Ter aanvulling, extra informatie:

- Qixium met de daarop actief zijnde modules is als 1 centraal SaaS-systeem actief. Hoewel veel zaken gelogd worden is dit niet geschikt als forensisch bewijs.
- Logging van gebruik van accounts binnen de Microsoft omgeving van de klant valt buiten ons zichtveld.
- Logging van ORB zelf is toegankelijk voor de ORB-beheerder vanuit de klant.
- Voor inloggen op de Qixium ORB toepassing kan MFA worden ingesteld
- Qixium ondersteund ook SSO (kan extra kosten aan het platform tot gevolg hebben)
- Uiteraard wordt alle gevoelige data door middel van encryptie opgeslagen

Beknopt kan het gebruik van het account vanaf de kant van de klant strikt beperkt worden tot de ORB-toepassing zelf, ORB is hard-coded beperkt in de te verwerken data, er kan worden toegezien op de activiteiten van het account, de SaaS omgeving is zowel veilig op gebied van inloggen, de data die privacy technisch van belang is binnen ORB en is beperkt tot de organisator en deelnemers email adressen, het onderwerp en eventueel de body van de reservering. De body kan echter vanaf de Exchange/O365 kant door de klant zelf niet beschikbaar worden gemaakt.

Hierdoor kan de informatie die uitgewisseld wordt, beperkt worden tot het onderwerp, de organisator en deelnemers emailadressen en de datum en tijdstippen van de reservering. De data, wordt zowel in transitie als bij opslag beveiligd door middel van encryptie.