# Authenticatie Onderzoek



Sjoerd Burhenne & Joost Raemakers

Inhoudsopgave

[Authenticatie Onderzoek 1](#_Toc153990536)

[1. Voorwoord 3](#_Toc153990537)

[2. Inleiding 3](#_Toc153990538)

[2.1 Probleemdefinitie 3](#_Toc153990539)

[2.2 Hoofdvraag 3](#_Toc153990540)

[2.3 Deelvragen 3](#_Toc153990541)

[3. Onderzoeksmethode 3](#_Toc153990542)

[4. Op welke manieren kunnen externe partijen betere beveiligingsprotocollen bieden dan interne systemen? 3](#_Toc153990543)

[5. Welke verbeteringen of risico's brengt dit met zich mee voor de bescherming van gevoelige informatie? 4](#_Toc153990544)

[6. Welke gespecialiseerde kennis en tools kunnen externe partijen bieden die intern mogelijk ontbreken? 4](#_Toc153990545)

[7. Conclusie 4](#_Toc153990546)

[8. Bronnen 5](#_Toc153990547)

## 1. Voorwoord

Voor ons schoolproject genaamd 'Volunteer' willen we gebruikersauthenticatie implementeren. We vroegen ons af wat hiervoor een makkelijke en veilige manier is. We ontdekten dat er veel verschillende bedrijven zijn die dit voor je kunnen doen. Daarom willen we onderzoek doen naar de veiligheid en het gebruik van deze tools. We voeren dit onderzoek uit voor semester 3 van de opleiding Software Development aan Fontys HBO ICT.

## 2. Inleiding

### 2.1 Probleemdefinitie

Het uitbesteden van authenticatie aan externe partijen is een groeiende trend binnen organisaties, maar roept belangrijke vragen op over de impact ervan op de veiligheid, efficiëntie en gebruikerservaring. Het fundamentele probleem dat moet worden onderzocht, betreft de balans tussen de voordelen en nadelen van het gebruik van externe partijen voor authenticatieprocessen.

### 2.2 Hoofdvraag

Wat zijn de voornaamste voordelen en nadelen van het uitbesteden van authenticatie aan externe partijen, en hoe beïnvloeden deze factoren de veiligheid, efficiëntie en gebruikerservaring binnen het project?

### 2.3 Deelvragen

* Op welke manieren kunnen externe partijen betere beveiligingsprotocollen bieden dan interne systemen?
* Welke verbeteringen of risico's brengt dit met zich mee voor de bescherming van gevoelige informatie?
* Welke gespecialiseerde kennis en tools kunnen externe partijen bieden die intern mogelijk ontbreken?

## 3. Onderzoeksmethode

Voor dit onderzoek is het Development Oriented Triangulation framework, oftewel het DOT-framework, gebruikt. Het DOT-framework helpt bij het structureren van het onderzoek en de manier waarop de bevindingen worden gecommuniceerd. Het DOT-framework bestaat uit drie niveaus: what, why en how.

## 4. Op welke manieren kunnen externe partijen betere beveiligingsprotocollen bieden dan interne systemen?

Externe beveiligingsbedrijven zijn gespecialiseerd in het leveren van beveiligingsdiensten en beschikken over veel expertise en ervaring. Ze richten zich volledig op het begrijpen en oplossen van beveiligingsproblemen, wat anders is dan wanneer je dit intern zou doen, aangezien je dan een heel project moet onderhouden. Hierdoor is het mogelijk dat je niet altijd voldoende tijd kunt besteden aan het beveiligen van authenticatie wanneer je dit intern beheert. Een extern beveiligingsbedrijf kan zich daarentegen volledig richten op de dienst die ze aanbieden. Dit stelt hen in staat om up-to-date te blijven met de nieuwste tools en methoden. Externe partijen monitoren voortdurend bedreigingen en incidenten, waardoor ze snel kunnen reageren en problemen zonder onderbrekingen kunnen oplossen. Bovendien voeren ze onafhankelijke beoordelingen uit zonder de mogelijke vooroordelen die interne teams kunnen hebben. Wanneer je de authenticatie intern beheert, kun je deze precies afstemmen op het systeem en ben je onbeperkt in de mogelijkheden (Stech, 2021).

## 5. Welke verbeteringen of risico's brengt dit met zich mee voor de bescherming van gevoelige informatie?

Het uitbesteden van authenticatie betekent dat een organisatie afhankelijk is van derden. Als die partij fouten maakt of uitvalt, kan dit de toegang tot systemen belemmeren. Dit is natuurlijk niet gunstig voor zowel de organisatie als de gebruikers van het systeem. Bovendien worden mogelijk gevoelige inloggegevens opgeslagen. Als er een datalek of beveiligingsincident optreedt bij de externe partij, kan dit leiden tot de blootstelling van vertrouwelijke gegevens. Niettemin is de kans dat dit gebeurt over het algemeen kleiner dan wanneer je zelf de vertrouwelijke gegevens beheert (Stech, 2021). Het uitbesteden van authenticatie aan derden brengt ook kosten met zich mee. Het is belangrijk om hier zorgvuldig en verantwoordelijk naar te kijken, zodat er geen onverwachte kosten ontstaan.

## 6. Welke gespecialiseerde kennis en tools kunnen externe partijen bieden die intern mogelijk ontbreken?

Externe partijen hebben ervaring met het implementeren en integreren van authenticatiesystemen in diverse omgevingen, waardoor ze mogelijk beter zijn toegerust om complexe systemen op te zetten. Zo zijn ze vaak goed op de hoogte van de regelgeving en compliance-vereisten, wat essentieel is voor het correct implementeren van beveiligingsprotocollen en het voldoen aan wet- en regelgeving. Je hoeft dus niet zelf alle regelgevingen te kennen en laat het over aan derden met de kennis om het voor jou te doen (Glynn, 2018). Door middel van het uitbesteden van authenticatie kan je de aansprakelijkheid van datalekken verminderen en dus je reputatie beschermen (Stech, 2021).

## 7. Conclusie

De overweging om authenticatie uit te besteden aan externe partijen is een complexe kwestie met zowel voordelen als nadelen. De juiste keuze verschilt per organisatie en per project. Externe beveiligingsbedrijven bieden onmiskenbaar expertise, up-to-date kennis en gespecialiseerde middelen voor het implementeren van beveiligingsprotocollen. Hun focus op beveiliging als hoofdactiviteit en het vermogen om onafhankelijke beoordelingen uit te voeren, kan resulteren in een betere bescherming tegen bedreigingen en een meer proactieve aanpak van beveiligingsincidenten. Echter maakt dit je wel afhankelijk van derden, waardoor je vatbaar kunt zijn voor mogelijke uitval of fouten. De keuze om authenticatie uit te besteden is een moeilijke overweging waarbij naar de voor- en nadelen moet worden gekeken. “Volgens een Auth0-enquête uit 2020 onder IT-professionals besteedt momenteel 58% van hen authenticatie uit bij het bouwen van applicaties” (Gontovnikas, 2021). Daarom hebben we voor ons project besloten om de authenticatie uit te besteden aan een externe partij.

## 8. Bronnen

Stech, J. (2021, 20 januari). Why Outsource Your Auth System? FusionAuth. <https://fusionauth.io/blog/why-outsource-auth>

Glynn, S. (2018, 25 oktober). Becoming compliant with GDPR: Outsource or in-house? Code in Motion. <https://codeinmotion.ie/gdpr-compliance-outsource-or-inhouse>

Gontovnikas, M. (2021, 8 juni). What is IAM? Auth0. <https://auth0.com/blog/what-is-iam>