Detectie en Respons

Logging en Monitoringplan



Anthony Delgado, Ayoub Lfatmi, Per Taffijn en Mustafa Warsame

Datum:

*13 November 2023*

Deskundige docenten(en):

*H. Middelkoop en P. van den Bosch*

PDP-coach(es):

*M. Dijkstra*

# Inhoudsopgave

**Wet- en regelgeving****2** Algemene Verordening Gegevensbescherming (AVG) 2  
 Telecommunicatiewet 2  
 Wet op inlichtingen- en veiligheidsdiensten (WiV) 3

**Logging 3**

Welke onderdelen gaan we loggen? 3  
 Hoelang bewaren de logbestanden? 4  
 Op welke manier kan logging plaatsvinden?4

**Detectie en Respons** [**5**](https://docs.google.com/document/d/1-5DWf6y_nqeJdPBpw62jO6yLJub4ZLKNVxVxcSYEmdc/edit#heading=h.pz4fycedwaob)Rollen 5  
 Roles and Permission matrix 6

Alert Triggers 6  
  
**Literatuurlijst****7**

# Wet- en regelgeving

Algemene Verordening Gegevensbescherming (AVG)

De AVG is de Europese wetgeving die gaat over gegevensbescherming. Het bepaalt met name de werving en beperking van persoonsgegevens. de AVG legt een aantal restricties op het loggen en monitoren van persoonsgegevens. Bedrijven hebben bijvoorbeeld expliciete toestemming nodig voordat zij persoonsgegevens mogen verzamelen. Verder is het van belang dat alleen de gegevens verzameld worden die noodzakelijk zijn voor een bepaald doel. En bedrijven moeten ook aan particulieren kunnen verantwoorden waarom bepaalde gegevens verzameld worden.

Telecommunicatiewet

De telecommunicatiewet richt zich meer op het verwerken van persoonsgegevens in de elektronische communicatiesector. Dit kan van toepassing zijn op het loggen en monitoren van communicatie zoals bijvoorbeeld telefoongesprekken en chat.

Wet op inlichtingen- en veiligheidsdiensten (WiV)

Deze wet richt zich op de bevoegdheden van de Nederlandse inlichtingen- en veiligheidsdiensten. Het heeft betrekking op het verzamelen van gegevens voor de nationale veiligheid en defensie. Het gebruik van bepaalde monitoringstechnieken kan onder deze wet vallen.

# Logging

Welke onderdelen gaan we loggen?

1. **Inlogacties:**

Waarom loggen? Inlogpogingen geven inzicht in wie toegang probeert te verkrijgen tot de webapplicatie. Dit is van belang voor beveiligingsdoeleinden en kan helpen bij het detecteren van ongeautoriseerde toegang. Wij zullen ook kijken waar deze inlogpogingen vandaan komen en verdachte landen zoals Rusland blokkeren.

1. **Wijzigingen in rechten:**

Waarom loggen? Het bijhouden van wijzigingen in gebruikersrechten is essentieel voor het beheren van de toegangscontrole. Dit kan helpen bij het identificeren van ongeautoriseerde wijzigingen en bij het oplossen van problemen met de toegangsrechten van gebruikers. Denk hierbij bijvoorbeeld aan iemand die ineens een beheerder is geworden zonder enige controle van iemand.

1. **Toegang tot gevoelige gegevens:**

Waarom loggen? Loggen van toegang tot gevoelige gegevens, vooral die van panelleden met een beperking, is van vitaal belang voor privacy en naleving van wet- en regelgeving. Dit helpt ook bij het identificeren van ongeoorloofde toegang.

1. **Belangrijke configuratiewijzigingen:**

Waarom loggen? Als er configuratiewijzigingen plaatsvinden, zoals aanpassingen aan de database-instellingen of API-configuraties, is het van belang om deze wijzigingen vast te leggen. Dit helpt bij het beheer van het systeem en bij het oplossen van problemen.

1. **Fouten en waarschuwingen:**

Waarom loggen? Registreren van fouten en waarschuwingen helpt bij het actief identificeren en aanpakken van potentiële problemen in de applicatie. Dit is van belang voor zowel beveiligingsdoeleinden als voor het verbeteren van de gebruikerservaring. Denk hierbij aan loggen hoe vaak en welke foutmelding optreedt

1. **Uitschrijving uit een onderzoek:**

Waarom loggen? Op het moment dat een gebruiker zich uitschrijft uit een onderzoek is dat handig om te weten, voor zowel bedrijven als ons. Om bijvoorbeeld te kijken hoe vaak dit gebeurt of op wat voor onderzoeken het meest.

1. **Aanmeldingen en activiteiten van beheerders:**

Waarom loggen? Het bijhouden van aanmeldingen en activiteiten van beheerders is cruciaal om te weten wie toegang heeft tot het beheerdersportal en welke acties zij uitvoeren. Dit draagt bij aan de beveiliging van het systeem. Wederom zullen we natuurlijk verdachte accounts of accounts die niet op het bedrijfsportaal horen blokkeren.

1. **Wijzigingen in profielinformatie:**

Waarom loggen? Registreren van wijzigingen in profiel informatie, zoals contactgegevens of type beperking, is belangrijk voor het bijhouden van de juistheid van de gegevens en het identificeren van ongeautoriseerde wijzigingen.

Hoe lang bewaren we de logbestanden?

De meeste bedrijven hanteren een vuistregel met betrekking tot de bewaartermijn van logbestanden. Over het algemeen wordt er aangeraden logbestanden minimaal 90 dagen te bewaren. Hoe lang je na die 90 dagen logbestanden kan bewaren, hangt af van een aantal situaties. Bijvoorbeeld om welk type gegevens het gaat, opslagcapaciteit en kosten die het met zich mee zal brengen, incident- response tijdlijn etc. Door deze factoren samen is het dus lastig te zeggen hoelang wij precies de logbestanden precies gaan opslaan. Wel zullen wij een minimumtijd hanteren van 90 dagen.

Op welke manier kan logging plaatsvinden?

Er zijn heel veel verschillende manieren om monitoring te doen. We zullen er een paar noemen die van belang zijn voor de bovenstaande dingen die we willen loggen. Er zijn talloze plugins en applicaties die je kunt gebruiken om je applicatie te monitoren. Dit is handig voor ons zodat we niet alle functionaliteiten zelf in hoeven te bouwen.

**Inlogacties:**

Monitoring Tool: Auth0 of Okta.

Functionaliteit: Log alle inlogpogingen, inclusief mislukte pogingen, en ontvang meldingen bij verdachte activiteiten, zoals meerdere mislukte inlogpogingen binnen korte tijd. Dit sluit goed aan bij wat wij willen monitoren.

**Toegang tot gevoelige gegevens:**

Monitoring Tool: Database Activity Monitoring (DAM) tools zoals IBM Guardium of Imperva. Functionaliteit: Log en analyseer alle toegangspogingen tot gevoelige gegevens in de database, inclusief wie toegang heeft gehad tot welke gegevens.

**Beheerders- en Gebruikersactiviteit Monitoring:**

Monitoring Tool: Audit logs in AWS CloudWatch of Azure Monitor.

Functionaliteit: Log alle activiteiten van beheerders en belangrijke gebruikersinteracties.

Dit zijn enkele monitoring tools die gebruikt kunnen worden voor monitoring bij onze applicatie, sommige dingen kunnen wij zelf proberen in te bouwen. Indien dit niet lukt is het een optie om weer te kijken voor eventuele third party applicaties.

# Detectie en Respons

Rollen binnen de webapplicatie

Voor de applicatie van Stichting Accessibility zijn een aantal rollen opgesteld. De rollen zijn gemaakt op basis van de informatie uit de aangeleverde case op Brightspace. Ook hebben we onderzoek gedaan naar bepaalde rol-managmentsystemen van andere applicaties, en hoe zij hun rollen systeem hebben opgedeeld en geconfigureerd binnen de webapplicatie. Daarnaast hebben we ook voldoende literatuur op het internet hiervoor geraadpleegd (*zie* [*literatuurlijst*](#_h84o8jhvtyke)***)***

| **Naam Rol** | | **Taak** | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Ervaringsdeskundige | | *Eigen profiel aanmaken, wijzigen en verwijderen. Onderzoekenuitnodigingen lezen. Deelnemen aan onderzoeken. Chatten met bedrijven.* | | | | | |
| Bedrijf - Contactpersoon | | *Vertegenwoordigt een bedrijf dat op zoek is naar deelnemers voor bepaalde onderzoeken. Heeft toegang tot de bedrijvenportal om opdrachten te plaatsen, te chatten en resultaten van trackingstudies te publiceren/bekijken* | | | | | |
| Accessibility - Admin | | *Verantwoordelijk voor het algemene beheer van de applicatie. Heeft toegang tot de beheerdersportal voor het uitzetten van onderzoeken, koppelen van bedrijven en het beheren van gebruikersgegevens. Zorgt er ook voor dat de webapplicatie voldoet aan de toegankelijkheidsnormen.* | | | | | |
| Database Manager | | *Verantwoordelijk voor het beheer van de database waarin de gegevens van ervaringsdeskundigen, bedrijven, onderzoeken en dergelijke worden opgeslagen. Zorgt voor gegevensintegriteit, database-optimalisatie en beheert de toegangsrechten* | | | | | |
| Onderzoeksopstelling | | *Onderzoeken in de webapplicatie aanmaken en wijzigen.* | | | | | |
| Systeembeheerder | | *Verantwoordelijk voor het algemene systeembeheer van de webapplicatie. Handelt technische problemen af, beheert serverprestaties en zorgt voor de systeembeveleiging.* | | | | | |
| Back-end developer | | *Verantwoordelijk voor het bouwen, testen en bijhouden van de applicatie.* | | | | | |
| Webontwikkelaar | | *Vervullen taken zoals het ontwerpen en implementeren van de gebruiksinterfaces. Daarnaast zorgt een webontwikkelaar ook voor de verwerking en opslag van gegevens* | | | | | |
| Security Analyst | | *Verantwoordelijk voor het bewaken van de beveiliging van de applicatie en het bekijken en afhandelen van security alerts.* | | | | | |

Roles and Permission Matrix

<https://docs.google.com/spreadsheets/d/1VXCv3PX0j4Ks7nr4XFBhEKm3fH91Y_mP8m1K3-15da8/edit?usp=sharing>

Alert Triggers

<https://docs.google.com/spreadsheets/d/1VXCv3PX0j4Ks7nr4XFBhEKm3fH91Y_mP8m1K3-15da8/edit?usp=sharing>

# Literatuurlijst

7 Essential roles in a web development team - AmeXio. (2023, 31 augustus). AmeXio. <https://www.amexio.fr/en/2023/08/25/7-essential-roles-in-a-web-development-team/>

Schoffelmeer, M. (2021, 9 december). Implementing role based security in a web app - BlueCore Engineering - Medium. Medium. <https://medium.com/bluecore-engineering/implementing-role-based-security-in-a-web-app-89b66d1410e4>

Ellingwood, J. (2017, 5 december). An introduction to metrics, monitoring, and alerting. DigitalOcean. <https://www.digitalocean.com/community/tutorials/an-introduction-to-metrics-monitoring-and-alerting>