Secure Software Toetsing (samenvatting)

Schuldenknooppunt

in opdracht van

NVVK

NVVK-Schuldenknooppunt-REPORT-v1.0.pdf
Tim Hemel, MSc.
Versie 1.0
18 juni 2020

VERTROUWELIJK

Secura BV
Vestdijk 59
5611 CA EINDHOVEN
The Netherlands

Karspeldreef 8
1101 CJ AMSTERDAM
The Netherlands

T +31 (0)40 23 77 990

E info@secura.com

W https://www.secura.com

DOCUMENT MANAGEMENT

Reviewers

Naam	Functie	Datum	Versie

Wijzigingen

Versie	Datum	Initialen	Aanpassingen
0.1	2020-06-08	TH	Initiële versie
1.0	2020-06-18	TH	Definitieve versie

INHOUDSOPGAVE

1. MANAGEMENTSAMENVATTING

Dit rapport beschrijft de resultaten van een toetsing van de software voor het Schuldenknooppunt van NVVK. Dit onderzoek is gestart op 14 april 2020 en uitgevoerd door Tim Hemel.

1.1. Aanleiding van het onderzoek

NVVK ontwikkelt het zogenaamde Schuldenknooppunt, een systeem waarmee schuldhulpverleners en schuldeisers berichten over schuldenaars kunnen uitwisselen en afspraken kunnen maken. Omdat het hier persoonsgegevens betreft, is de bescherming hiervan uitermate belangrijk. Het bedrijf Innovadis implementeert dit schuldenknooppunt.

Op 26 maart 2020 hebben de heer van de Ven van NVVK en Ronald Meyer en Tim Hemel van Secura met elkaar gesproken. Het onderwerp van dit gesprek was de behoefte van NVVK aan hulp tijdens het realiseren van het schuldenknooppunt, in de vorm van toetsing en begeleiding. Secura heeft hiervoor een offerte uitgebracht met referentie '20030269-NVVK-Consultancy Schuldenknooppunt FINAL'.

1.2. Doel

Het begeleidings- en toetsingstraject heeft als doel beveiligingsproblemen vroegtijdig vast te stellen en om in overleg met Innovadis oplossingen te bespreken. Om belangenverstrengeling te voorkomen, beperkt Secura zich hierbij tot het noemen van standaardoplossingsrichtingen, of het beoordelen van oplossingen die Innovadis bedenkt.

De begeleiding en toetsing richt zich op alle relevante fases van het softwarevoortbrengingsproces, in dit geval requirements, architectuur en code. Tussen de start van het traject en de opleverdatum van het schuldenknooppunt was niet veel tijd, daarom ligt de focus op de beveiliging van de op te leveren software en valt hoe Innovadis beveiliging in het ontwikkelproces heeft ingebed, hoe zij beveiliging in het product test en hoe zij de operationele beveiliging regelt buiten de scope van het traject.

1.3. Aanpak

Secura volgt een aanpak gebaseerd op het 'Framework Secure Software'[1], dat zich specifiek richt op het inzichtelijk maken van beveiliging in een product, door van alle fases van de ontwikkeling opgeleverde resultaten te bekijken. Concreet houdt dit in dat we hebben gekeken naar security requirements, bedreigingen inherent aan de architectuur hebben gezocht, broncode hebben gereviewd en een korte pentest hebben uitgevoerd op het draaiende systeem. De toetsing is breder dan enkel een pentest, wat ons in staat stelt de beveiliging effectiever te beoordelen.

1.4. Resultaten

1.4.1. Over de toetsing

Deze toetsing kan gezien worden als een eerste meetmoment om een indruk te krijgen van de beveiliging van de code. Vanwege het relatief korte tijdsbestek van het onderzoek is gekozen voor een meer ad-hoc aanpak, teneinde zoveel mogelijk belangrijke problemen te detecteren in de software voor de eerste release. Om een constant niveau van beveiliging te krijgen en te houden is het belangrijk op continue basis aandacht te besteden aan beveiliging in het software-ontwikkelproces.

Secura BV baseert zich hiervoor op het SAMM model van OWASP. Dit is een verzameling van activiteiten tijdens het softwareontwikkelproces die de beveiliging verhogen. SAMM organiseert deze activiteiten volgens de verschillende fases van ontwikkeling: ontwerp, implementatie, verificatie, operations en governance. Binnen deze fases maakt SAMM onderscheid in verschillende volwassenheidsniveaus. Daarmee kan men meten en doelen bepalen voor een verbeteringspad.

Binnen het schuldenknooppunt zien we als eerste concrete stappen in deze richting het analyseren van user stories om te kijken welke beveiligingsproblemen men hier kan verwachten. Uit dit traject hebben we geleerd dat wanneer het ontwikkelteam zich bewust is van de mogelijke problemen, ze hierover nadenken en een oplossing implementeren. De grootste winst is dus te behalen in de bewustwording van mogelijke beveiligingsproblemen en bijbehorende oplossingen.

[1] https://www.securesoftware.nl/resources/FrameworkSecureSoftware_v1.pdf

Daarnaast is het belangrijk de implementatie hiervan te blijven controleren, maar dat zal met deze voorbereidende activiteiten veel effectiever kunnen.

1.4.2. Bevindingen

Een deel van de gevonden bevindingen is verholpen en bij een tweede review konden we concluderen dat de bedreiging hiermee was weggenomen. Na het bespreken van deze bevindingen bleek dat van veel bevindingen het risico acceptabel was en dat voor andere bevindingen een oplossing wordt of is geïmplementeerd. Een tweetal bevindingen verdient nader onderzoek, maar het risico hiervan is geen showstopper voor de eerste livegang.

1.4.3. Overige aanbevelingen

Niet alle beveiliging is volledig in handen van NVVK of Innovadis. Aansluitende partijen kunnen ook beveiligingsfouten maken of bedreigingen over het hoofd zien. In dat kader is het handig een set beveiligingseisen voor aansluitende partijen op te stellen, zodat ook duidelijk is welke beveiligingsverwachtingen en -verantwoordelijkheid waar liggen.

1.5. Eindconclusie

Dit onderzoek was slechts een momentopname van een veranderend systeem en de diepgang van het onderzoek was beperkt door beschikbare tijd. Dit rapport geeft geen garantie dat het schuldenknooppunt vrij is van kwetsbaarheden.

Binnen het kader van het uitgevoerde onderzoek, hebben we, na het bespreken van bevindingen en controle van aanpassingen in het systeem, in onze ogen geen serieuze beveiligingsproblemen kunnen vaststellen.