Solution Intent

IAM BINNEN MICROSERVICES

Finn Alberts, Lorenzo Clermonts, Giorgio Peerboom,
Bram Verheijen en Erik Wingers
ZUYD HOGESCHOOL | HBO ICT

Inhoud

1 Inleiding

Waar vroeger applicaties voornamelijk monolithisch ontwikkeld werden, wordt tegenwoordig steeds meer gekozen om applicaties modulair te ontwikkelen. Zo worden applicaties steeds meer ontworpen en gebouwd als een verzameling samenwerkende microservices. Binnen een monolithisch systeem zitten alle functionaliteiten in één applicatie. Bij microservices worden deze functionaliteiten juist opgesplitst in kleine stukjes waarbij elke microservice zich focust op een specifieke functionaliteit. Elke microservice kan hierdoor onafhankelijk van elkaar functioneren. Deze microservice-architecturen worden ook steeds vaker in de cloud gedeployed.

Bij deze monolithische systemen vond de authenticatie en autorisatie vaak maar één keer plaats bij het binnenkomen van systeem. Zodra de gebruiker binnen was, was het niet meer nodig om telkens opnieuw te authentiseren en autoriseren. Bij een microservice-architectuur is dit een stuk complexer, omdat het systeem over verschillende services verdeelt is, waarbij authenticatie en autorisatie telkens opnieuw in acht moet worden genomen.

2 Doel

Het doel is om voor een microservice-architectuur in de cloud middels Kubernetes onderzoek te doen naar oplossingen voor de uitdagingen die ontstaan met betrekking tot security. Eén van de grotere uitdagingen hierbij is authenticatie en autorisatie. Hierbij moet worden gekeken naar hoe kan worden gewaarborgd dat een digitale identiteit constant integer geauthentiseerd is en alleen de mogelijkheid heeft om acties uit te voeren, waarvoor deze is geautoriseerd. Een extra uitdaging hierbij is dat rekening moet worden gehouden met het feit dat microservices ook regelmatig elkaar aanroepen. Hierbij moet worden gezorgd dat een gebruiker niet indirect een microservice kan benaderen, waarvoor hij geen toegang heeft, via een andere microservice waarvoor hij wel geautoriseerd is.

Andere belangrijke aspecten zijn het beveiligen van data (en daarbij ook kijkende naar privacy), audits en het onderzoeken van de algehele risico’s die hierbij komen kijken.

Om dit onderzoek tastbaar te maken wordt gebruik gemaakt van een praktisch voorbeeld: een vaccinatieregister. Dit wordt gedaan om de verschillende beveiligingsaspecten te demonstreren. Een vaccinatieregister heeft als voordeel dat er veel verschillende rollen bij betrokken zijn, zoals huisarts, burger, vaccinatiecentrummedewerker. Deze rollen hebben allemaal verschillende rechten binnen het systeem. Hierbij ligt de focus in eerste instantie op applicatieniveau en kan worden verlengd naar platformniveau.