Uitbreiding van het External Attack Surface Management voor Baloise

Reflectie

Bachelor in de Elektronica-ICT
keuzerichting Cloud

Tuur Hulselmans

Academiejaar 2024-2025

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

Inhoud

1 INTRODUCTIE

In dit reflectiedocument blik ik terug op mijn stageperiode van dertien weken bij Baloise. Tijdens mijn stage heb ik gewerkt aan het opzetten van een geautomatiseerd monitoringsysteem voor publieke en interne webapplicaties, met als doel de beveiliging hiervan te verbeteren. Dit project omvatte verschillende fasen, waaronder het analyseren van bestaande applicaties, het implementeren van monitoring- en vulnerability scanning tools, en het automatiseren van processen via Azure DevOps.

Dit document is opgedeeld in twee hoofdonderdelen. Ten eerste geef ik een inhoudelijke reflectie waarin ik beschrijf wat ik concreet heb gerealiseerd, welke stappen nog afgerond moeten worden en welke impact mijn werk heeft op de organisatie. Ten tweede volgt een persoonlijke reflectie, waarin ik mijn leerproces toelicht, de competenties die ik heb ontwikkeld en de uitdagingen die ik ben tegengekomen en heb overwonnen.

Met deze reflectie wil ik een helder beeld schetsen van mijn bijdrage aan Baloise en mijn persoonlijke groei gedurende deze stageperiode. De lezer krijgt zo inzicht in zowel het technische als het persoonlijke aspect van mijn ervaring.

2 INHOUDELIJKE REFLECTIE

2.1 Gerealiseerd

Gedurende mijn stageperiode van dertien weken heb ik gewerkt aan het opzetten van een geautomatiseerd systeem voor het monitoren van publieke en deels ook interne webapplicaties. Dit project bestond uit meerdere fasen die elkaar logisch opvolgden.

Allereerst heb ik een grondige inventarisatie en analyse uitgevoerd van de bestaande webapplicaties. Hierbij maakte ik gebruik van eerder verzamelde gegevens door een vorige stagiair, gecombineerd met informatie uit publieke certificaatbronnen.

Met deze inventaris als vertrekpunt ben ik gestart met het opzetten van het monitoringplatform om zo de actieve websites en webapplicaties uit de inventaris te filteren. Ik heb een platform geïnstalleerd en geconfigureerd waarmee de beschikbaarheid van de webapplicaties automatisch wordt gecontroleerd. Vervolgens heb ik de geïdentificeerde domeinen toegevoegd aan het systeem, zodat deze continu worden gemonitord op beschikbaarheid en storingen. Dankzij deze opzet beschikt Baloise nu over een operationeel en overzichtelijk monitoringsysteem dat automatisch rapporteert bij uitval of verminderde bereikbaarheid van hun publieke webapplicaties.

Nadat ik een lijst had met al de actieve webapplicaties, heb ik een onderzoek gedaan naar geschikte vulnerability scanners. Bij deze selectie hield ik rekening met factoren zoals betrouwbaarheid, de reikwijdte van de scanmogelijkheden en de mate waarin de scanners geïntegreerd konden worden in de bestaande infrastructuur.

Na de keuze van de geschikte scanners heb ik deze geïmplementeerd en geconfigureerd, met als doel om periodiek kwetsbaarheden te detecteren zonder schade toe te brengen aan de productieomgevingen. Parallel hieraan heb ik gewerkt aan de opzet van een CI/CD-integratie via Azure DevOps, zodat het opzetten van de infrastructuur zoveel mogelijk geautomatiseerd kon verlopen.

Tot slot heb ik het volledige proces zorgvuldig gedocumenteerd. Deze documentatie omvatte onder andere de uitgevoerde analyse, de verkregen scanresultaten en aanbevelingen in de vorm van best practices voor toekomstig gebruik en verdere optimalisatie.

De resultaten van dit project leveren directe meerwaarde op voor Baloise. Enerzijds biedt het systeem een verbeterd inzicht in de beveiligingsstatus van de publieke webapplicaties. Anderzijds wordt het proces van vulnerability scanning grotendeels geautomatiseerd, wat de efficiëntie verhoogt en de werklast van het interne securityteam aanzienlijk verlaagt.

2.2 Statusrapport

Hoewel ik tijdens mijn stageperiode grote vooruitgang heb geboekt en de basisfunctionaliteit inmiddels operationeel is, blijven er nog enkele onderdelen die verdere uitwerking vereisen.

Ten eerste is het vulnerability dashboard nog niet helemaal gerealiseerd. Tijdens de laatste week van de stage heb ik samen met een collega een basis dashboard gemaakt. Dit gaf al een eerste beeld hoe de resultaten van de scanners kunnen worden geïntegreerd met powerBi. De connectie tussen de resultaten en het powerBi dashboard moet nog wel worden opgezet maar hiervoor heb ik wat aanbeveling gegeven zodat dit normaal makkelijker moet kunnen gaan.

Daarnaast is de koppeling tussen het monitoringsysteem en de verschillende scanners nog niet volledig geautomatiseerd. Op dit moment moet de lijst van actieve scanners met een python script uit de monitoringtool gehaald worden en daarna in de pipeline gekopieerd worden. Ook hier heb ik wat aanbeveling gedaan wat de volgende stappen kunnen zijn bijvoorbeeld een automatische systeem om de python code automatisch uit te voeren.

Deze openstaande punten zijn echter duidelijk in kaart gebracht en vormen een logische en haalbare volgende fase in het project. Tijdens mijn stage heb ik hiervoor aanbevelingen geformuleerd, zodat Baloise hiermee zelfstandig verder aan de slag kan.

3 PERSOONLIJKE REFLECTIE

3.1 Persoonlijke betekenis

De stage bij Baloise was voor mij een waardevolle leerervaring die verder ging dan enkel het uitvoeren van technische taken. Het was mijn eerste kennismaking met de manier waarop cybersecurityprocessen in een grote organisatie professioneel worden aangepakt. Ik kreeg de kans om te werken in een complexe, reële werkomgeving waar veiligheid, structuur en samenwerking centraal staan. Deze stageperiode heeft mijn interesse in cybersecurity niet alleen bevestigd, maar ook verdiept. Daarnaast heb ik ervaren hoe belangrijk het is om als IT-professional niet alleen technische kennis te hebben, maar ook communicatief sterk te zijn en zelfstandig verantwoordelijkheid op te nemen binnen een team.

3.2 Geleerde Lessen en Ontwikkelde Competenties

Tijdens mijn stage heb ik verschillende technische en niet-technische competenties ontwikkeld. Op technisch vlak leerde ik werken met vulnerabilityscanners en de integratie ervan in een CI/CD-pipeline via Azure DevOps. Ook heb ik ervaring opgedaan met het interpreteren van scanresultaten, het inschatten van risico's en het documenteren van het gehele proces op een gestructureerde manier.

Daarnaast heb ik mijn analytische vaardigheden versterkt door het grondig vergelijken van scanners en het afwegen van hun voor- en nadelen. Ook op het vlak van projectmatig werken ben ik gegroeid: ik leerde plannen, prioriteren en taken op een iteratieve manier aanpakken binnen een agile werkwijze.

Niet-technisch gezien heb ik mijn communicatievaardigheden aangescherpt, vooral bij het terugkoppelen van resultaten naar mijn stagebegeleiders en bij het formuleren van aanbevelingen voor toekomstige verbeteringen. Ook zelfstandig werken en verantwoordelijkheid nemen waren belangrijke onderdelen van mijn leertraject.

3.3 Persoonlijke Groei

Een van de belangrijkste punten waarin ik ben gegroeid, is het vermogen om zelfstandig een project vorm te geven, keuzes te onderbouwen en problemen proactief aan te pakken. Aan het begin van de stage was het uitdagend om te weten waar te beginnen en hoe ik impact kon maken binnen een bestaande organisatie. Naarmate het project vorderde, kreeg ik meer vertrouwen in mijn aanpak en durfde ik kritische vragen te stellen of verbetervoorstellen te doen. Ik ben gegroeid in het combineren van technische diepgang met een gestructureerde en resultaatgerichte aanpak.

3.4 Problemen en Oplossingen

De meeste technische problemen ondervond ik bij het opzetten van het monitoringplatform. In Azure zijn er namelijk verschillende soorten containers beschikbaar, elk met hun eigen eigenschappen en opslagmogelijkheden. Het bleek moeilijker dan verwacht om de juiste container te kiezen en correct te koppelen aan de juiste opslag.

Een concreet voorbeeld hiervan was dat na een herstart alle opgeslagen gegevens verdwenen waren. Dit maakte duidelijk dat de data niet persistent werd opgeslagen. Om dit probleem op te lossen, ben ik dieper in de documentatie gedoken om te achterhalen welke containerconfiguratie geschikt was om de gegevens blijvend op te slaan. Uiteindelijk is het gelukt om een stabiele oplossing te implementeren.

Tijdens de stage stuitte ik op verschillende uitdagingen. Een van de grotere struikelblokken was het configureren van de vulnerability scanner op een manier die veilig en effectief was, zonder negatieve impact op de productieomgevingen. Ik heb dit opgelost door tests te draaien in een gecontroleerde omgeving, veel documentatie te raadplegen en nauw overleg te houden met het ciso team.

Ook op communicatief vlak waren er uitdagingen. Het overbrengen van technische inhoud aan mensen met een GRC cybersecurity achtergronden vereiste duidelijke taal en het vermogen om te schakelen tussen detail en overzicht. Hierin heb ik veel bijgeleerd.