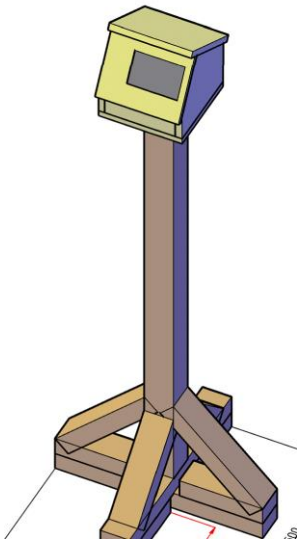
Beveiligingsplan – Project 56

Help de RDM-werkplaatsen om beter grip te krijgen op het gebruik van de werkplaatsen!



Projectleden:
- Matthijs Briel (0988991)
- Leandro de Nijs (1003440)
- Tom van Pelt (1003212)
- Gijs Kortlever (1003152)

Inleverdatum: 6 Februari 2022
Begeleiders: Erwin de Mos & S.M. Hekkelman
Bedrijfsbegeleider (Product Owner): F.W.J. Joosten Gladon
Gelegenheid: Eerste Kans

Inhoudsopgave

Hoofdstuk 1

Data Flow Diagram (DFD)

- Zie Bijlage 1.

Risicoanalyse algemeen / project specifiek

- In deze risicoanalyse wordt omschreven welke aanvallen (risico's) er mogelijk zijn en hoe deze uitgevoerd kunnen worden.

Algemeen

Nr.	Risico	Impact (1-5)*	Kans (1-5)*	Hoe te voorkomen en hoe op te lossen.
1	Componenten gaan kapot.	4	2	Kijken of er nog componenten zijn ter vervanging. Zo niet, dan de componenten bestellen. Komen de componenten niet binnen de huidige sprint aan, dan moet het door worden geschoven naar volgende sprint.
2	Componenten die besteld zijn komen niet op tijd aan.	3	2	Kijken of de sprint nog voltooid kan worden. Zo niet, dan moet het door worden geschoven naar volgende sprint planning.
3	Geen internetverbinding.	5	3	Er altijd rekening mee houden en dus belangrijke documenten downloaden in plaats van online te bekijken.
4	Tijdens een sprint erachter komen dat wat er in de sprint backlog staat voor de huidige sprint, niet haalbaar is in de tijd (die nog over is).	5	2	Kijken welke user story aangepast / eruit gehaald moet worden om de sprint wel haalbaar te maken.
5	Een projectlid wordt ziek.	3	2	Kijken wanneer het projectlid ziek is geworden. In het begin en kort ziek? -> dan is zijn deel nog haalbaar om te halen. In het midden/eind en langer ziek? -> Taakdeel verdelen over de andere projectleden.
6	Scholen gaan weer dicht i.v.m. nieuwe coronamaatregelen.	5	1	Kijken wat er thuis gedaan kan worden en kijken of er bij iemand (veilig) afgesproken kan worden om aan het project te werken.
7	Een projectlid stopt met de opleiding.	5	1	Taken van huidige sprint van stoppende projectlid verdelen over de rest van de projectleden. De andere projectleden moeten rekening houden met meer werk voor de rest van het project.

Project specifiek

Nr.	Risico	Impact (1-5)*	Kans (1-5)*	Hoe te voorkomen en hoe op te lossen.
1	Opdrachtgever is niet bereikbaar.	2	4	Vooraf informeren wanneer de opdrachtgever bereikbaar is en dus optimaal gebruik maken van de contact-momenten.
2	Budget raakt op.	5	2	Voorzichtig omgaan met de aankoop van componenten. En goed bijhouden wat en voor welke prijs we spullen hebben gekocht.
3	Stroom valt uit op de RDM	5	1	Hier kunnen wij niet zo veel aan doen, dit moet worden opgelost door de werknemers bij de RDM. Wel kunnen we een tijdelijke oplossing bedenken.
4	Internet valt weg op de RDM	4	3	Hier kunnen wij niet zo veel aan doen, dit moet worden opgelost door de werknemers bij de RDM. Wel kunnen we een tijdelijke oplossing bedenken.

* 1-5 = 1 is minst belangrijk, 5 is meest belangrijk

Legenda:

- Impact 1 = erg klein, heel erg makkelijk op te vangen als dit voorkomt
- Impact 5 = erg groot, moeten grote maatregelen worden genomen om dit probleem op te lossen
- Kans 1 = erg klein, komt eigenlijk niet voor, maar zou in theorie voor kunnen komen
- Kans 5 = erg groot, zeer aannemelijk dat dit voor kan komen tijdens een van de sprints

Attack Tree

- Zie Bijlage 2

Hoofdstuk 2

Beveiligingsrisico's

In onderstaande tabel staan de meest belangrijke en voorkomende beveiligingsrisico's.

Risico Nr.	Risico	Uitvoering Risico
1	Met requests naar de server is er toegang mogelijk naar de database.	Door URL's die niet gebruikt worden door de API te gebruiken kunnen er requests naar de serve gestuurd worden die niet gecheckt worden door de API.
2	Iemand kan bij de data in de database komen zonder de API te gebruiken.	Als er toegang is tot de bestanden hiërarchie van de server zou het bestand van database geopend kunnen worden.
3	Iemand kan zomaar de registratiepaal openmaken en bij de binnenkant komen.	Iemand kan bij de binnenkant komen door een plankje weg te trekken doordat deze niet goed vastzit. Ook kan er bijvoorbeeld nog een gat zitten in de behuizing waardoor er zeer gemakkelijk bij gekomen kan worden.
4	Iemand kan computer van de registratiepaal bedienen.	Iemand sluit een toetsenbord of muis aan via een usb-poort aan de binnenkant of buitenkant van de behuizing en kan zo de computer van de paal besturen en bijv. de registratie software (GUI) uitzetten of malware laten draaien.
5	Iemand kan een bar/QR-code scannen die malware bevat	Iemand scant een QR-code met bijv. een commando waarmee er data kan worden gestuurd naar de database die de database kan hacken.
6	Als iemand de juiste URL heeft van de API, kan deze zonder authenticatie de data inzien/versturen.	De URL is bekend bij iemand die hier eigenlijk niet tot geautoriseerd hoort te zijn. Deze persoon kan via deze URL de JSON-data uit de API ophalen en zelf weergeven.

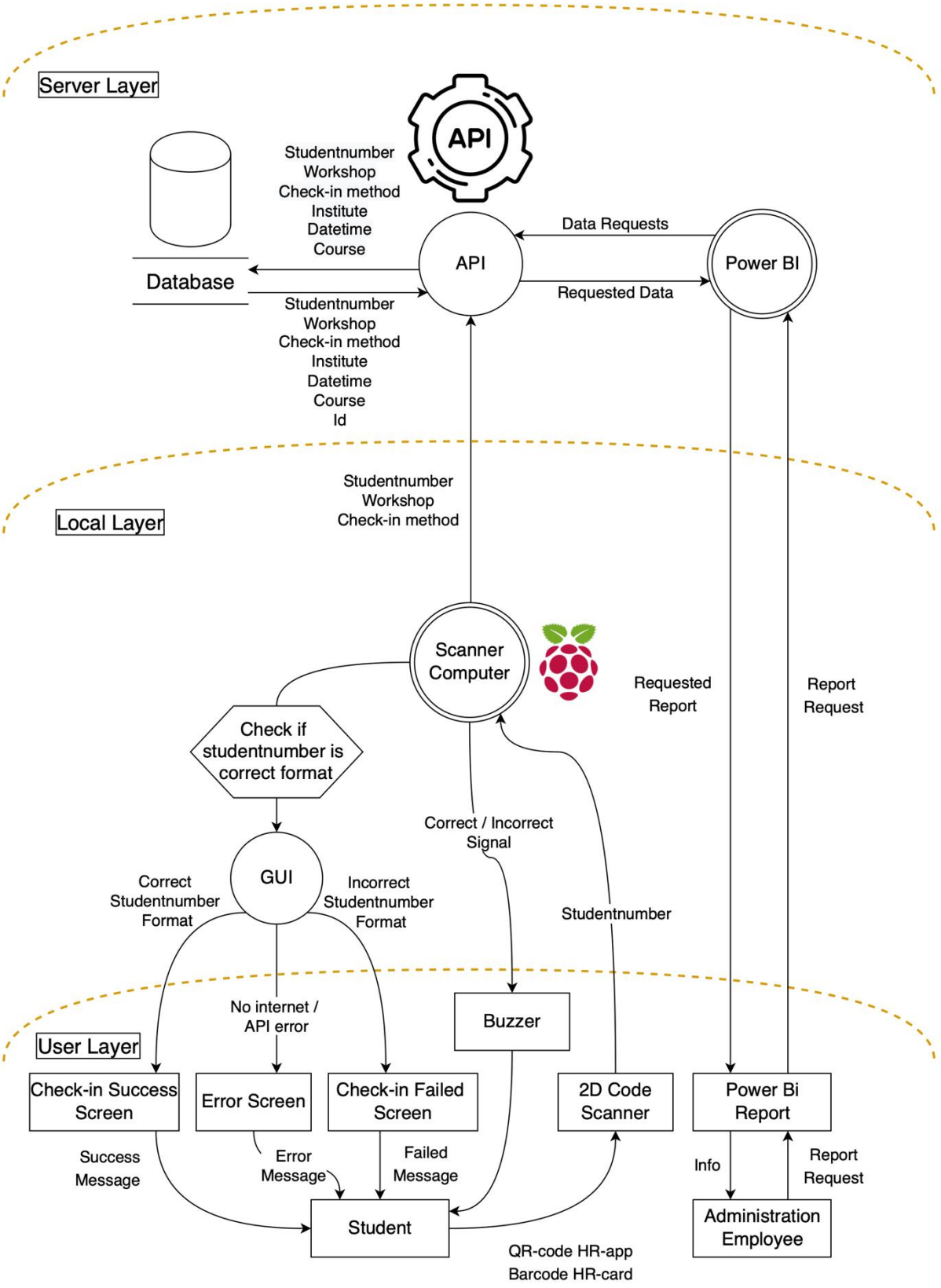
Maatregelen

In onderstaande tabel staan de maatregelen die genomen moeten worden om de beveiligingsrisico's zoveel mogelijk te verhelpen.

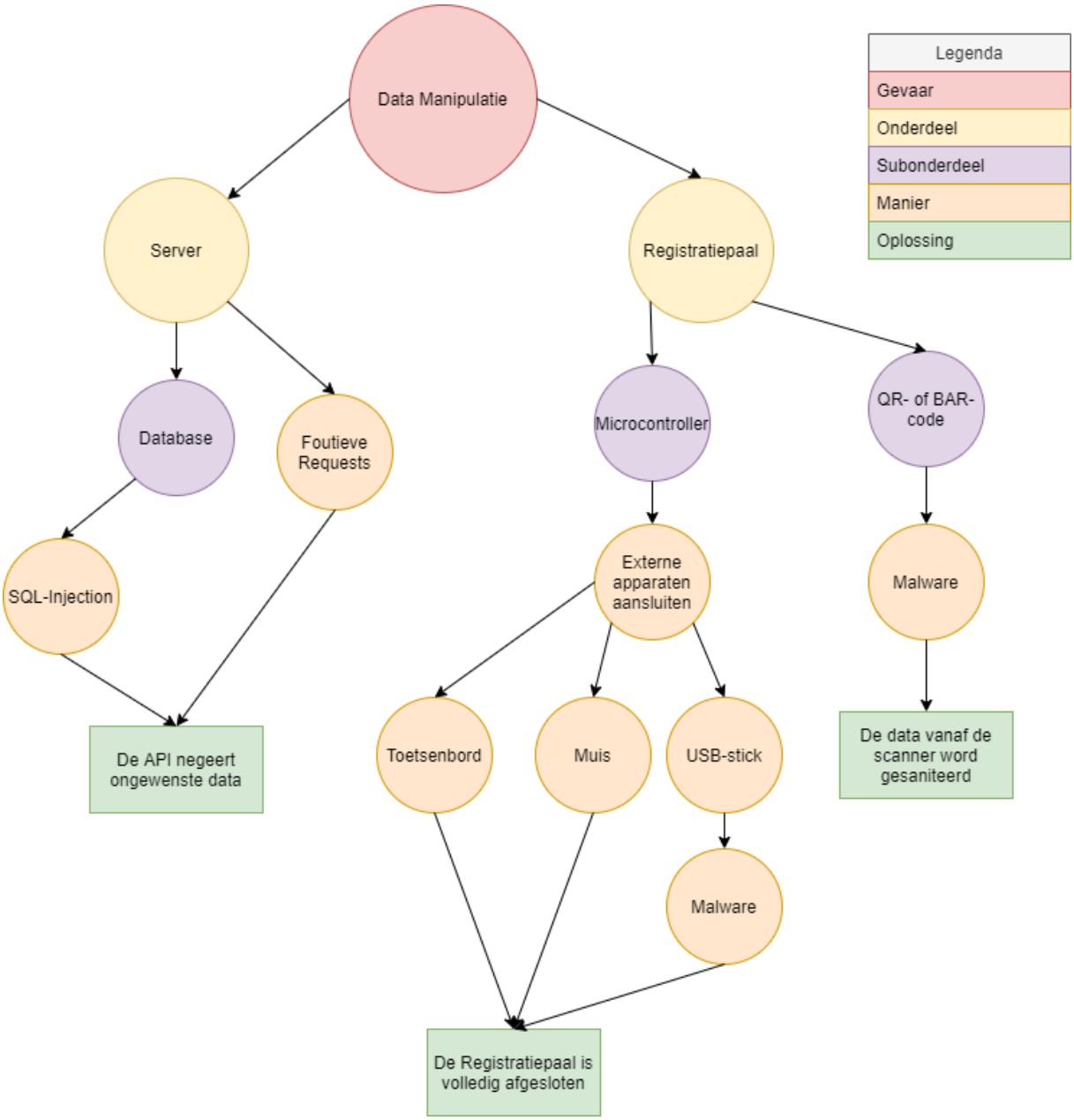
Risico Nr.	Maatregel Nr.	Maatregel
1	1	Specifieke URL's in de database die over bepaalde delen van de database gaan. Alle requests naar de server die niet gelijk zijn aan een van deze URL's worden genegeerd. Alleen POST en GET requests worden geaccepteerd. Vervolgens moet de URL ook kloppen met wat vastgelegd staat in de documentatie.
2	2	In de API wordt alleen data die gelijk is aan afgesproken formats herkend, alles dat niet volgens de documentatie correct is wordt genegeerd en weggegooid. Denk hierbij aan extra ongewenste data toevoegen achter een legitiem data format. Deze data worden genegeerd doordat alleen de data met het juiste voorvoegsel wordt gepakt en deze data ook nog wordt gecheckt of het bijvoorbeeld de juiste string lengte of zelfs juiste inhoud bevat. Dit alles om te zorgen zodat alleen gewenste data überhaupt dicht bij de database kan komen.
3	3	Het materiaal waarmee de registratiepaal wordt gemaakt is stevig en zit goed vastgeschroefd zodat er tenminste gereedschap aan toe moet komen om de registratiepaal open te maken. Eventueel kan het hout en de schroeven ook nog verlijmd worden zodat de registratiepaal niet meer uit elkaar te halen is. Als er gelijmd wordt is het aan te raden, om ergens een klepje te maken met een goed scharnier en slot erop zodat er toch nog bij de binnenkant gekomen kan worden, maar alleen door degenen die daartoe bevoegd zijn.
4	4	Er moeten geen USB-poorten zijn gemaakt aan de buitenkant zodat er bijvoorbeeld geen toetsenbord of muis kan worden aangesloten. Voor het prototype wat er bij dit project wordt opgeleverd is dit wel zo, omdat het heel handig is met testen. Ook moet de touchscreen uitstaan op het scherm. Dit is makkelijk door gewoon geen software te installeren op de Pi die ervoor zorgt dat de touchscreen werkt. Default werkt de touchscreen al niet namelijk.
5	5	In de software (GUI) van de registratiepaal moet worden gecheckt met bijvoorbeeld een if statement of de data die gescand wordt 7 tekens lang is en alleen uit cijfers bestaat. Dat is namelijk het format van een studentnummer. Daardoor kan er geen andere data dan alleen een studentnummer worden gestuurd naar de API.
6	6	Zelf geen maatregelen voor genomen, wel een aanbeveling.

Bijlagen

Bijlage 1 – Data Flow Diagram



Bijlage 2- Attack Tree



Changelog

Versie	Datum	Aanpassing	Auteur
1.0	15/12/2021	Eerste versie	Matthijs Briel
1.1	19/12/2021	Bijlage toegevoegd en kleine lay-out aanpassing	Tom van Pelt
1.2	15/01/2022	Afbeeldingen op Voorblad toegevoegd	Tom van Pelt
1.3	24/01/2022	Grote aanpassingen	Gijs Kortlever
1.4	26/01/2022	DFD aangepast naar nieuwe versie	Tom van Pelt
1.5	30/01/2022	Aanpassingen en grote aanvullingen	Tom van Pelt
1.6	31/01/2022	Aanvulling / aanpassingen	Leandro de Nijs & Tom van Pelt & Gijs Kortlever