|  |  |
| --- | --- |
| Beveiligingsplan | |
|  | |
| Cursuscode/Cursusnaam: TINPRJ0334/Project Bank  Versie: eerste versie  Product Owners: L. van Dam & W.B. Volders | Taylor Wernet - 0948313 **Connor Cullens -** 1011010 **Frank van Etten -** 1009269Marouan El Yachioui - 1014860 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | |  |  |
|  | InleidingDit verslag is geschreven om de verschillende elementen van de beveiliging van dit project in kaart te brengen. Hier wordt uitgelecht welke bedreigingen er voor kunnen komen aan de integriteit van de bank en hoe we de bedreigingen het beste kunnen oplossen. Bij de oplevering van de beveiligingsplan aan de opdrachtgever(Product Owner) laten we zien wat de risicofactoren zijn van de bank en welke maatregelen er genomen gaat worden om de risico’s op een effectieve manier te minimaliseren. | | |  |
|  |  |
|  |  | |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | DesignRisicoanalyse De risicofactoren die in de design kunnen voorkomen zijn:   * De hardware is blootgesteld waardoor een persoon het kan stuk maken of de hardware misbruiken. * Het geld is makkelijk bereikbaar waardoor een persoon er makkelijk bij kan komen en vervolgens stelen. * Het geldautomaat is zwak geconstrueerd waardoor een persoon het makkelijk stuk kan maken en bij het geld of hardware van de geldautomaat kan komen. | **Maatregelen**  De maatregelen die in de design genomen gaan worden zijn:   * Hardware wordt onbereikbaar gemaakt voor de gebruiker, door het te verbergen in de constructie. * Geld wordt onbereikbaar gemaakt voor de gebruiker, door het te verbergen in de constructie.   De constructie wordt van hout gemaakt zodat het stevig is. |  |
|  |  | |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | DatabaseRisicofactoren De risicofactoren die in de database kunnen voorkomen zijn:   * Iemand kan makkelijk in de database komen als de account niet goed beveiligd is. * De pincodes zijn zichtbaar in de database van de gebruikers. * Een gebruiker kan pincode eindeloos invoeren en het account wordt niet geblokkeerd. | **Maatregelen**  De maatregelen die in de database genomen gaan worden zijn:   * De database wordt beveiligd met accounts die alleen gebruikt mogen worden door de beheerder en product owner. Op deze manier weten alleen zij alleen de inlog gegevens en kunnen zij alleen bij de database komen. * De pincode wordt gehashed zodat niemand kan zien wat de pincode is. * Er wordt gekeken naar de aantal keren dat de pincode verkeerd is ingevoerd, na 3 keer fout invoeren wordt de pas geblokkeerd. |  |

## User interface

### Risicofactoren

De risicofactoren die in de user interface kunnen voorkomen zijn:

• De gebruiker kan de ingevoerde pincode zien op het scherm en dus ook de mensen die achter de gebruiker staan kunnen het op het scherm zien.

### Maatregelen

De maatregelen die in de user interface genomen gaan worden zijn:

• Op het moment dat de pincode wordt ingevoerd, het enigste dat de gebruiker op het scherm te zien krijgt zijn sterretjes zodat de pincode niet te zien is. Op deze manier is de pincode niet zichtbaar maar kan je wel zien hoeveel cijfers je hebt ingevoerd.