BEVEILIGINGSRAPPORT

Cursuscode/Cursusnaam: TINPRJ0334/Project Bank

Versie: eerste versie

Product Owners: L. van Dam & W.B. Volders

Naam	Studentennummer
Taylor Wernet	0948313
Connor Cullens	1011010
Frank van Etten	1009269
Marouan El Yachioui	1014860

Inhoud

Inleiding

Dit 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.

Design

Risicoanalyse

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.

Database

Risicofactoren

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.
- De sessie van de gebruiker blijft open na het pinnen.

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.
- De sessie van de gebruiker wordt per direct afgesloten als de gebruiker heeft gepind of als de gebruiker de sessie heeft afgebroken.

Server

Risicofactoren

De risicofactoren die in de user server kunnen voorkomen zijn:

- De verbinding tussen de client en server zijn makkelijk te bereiken omdat de verbinding niet beveiligd is.
- Als je de server wilt bereikt wordt het gedaan op een niet beveiligde verbinding bijv. Telnet.
- De server kan makkelijk binnengedrongen worden door een voorspelbare en makkelijke wachtwoord te gebruiken.
- De server kan makkelijk aangevallen worden door dat je niet bewust bent van welke poorten de aanvallen kunnen komen.

Maatregelen

De maatregelen die in de server genomen gaan worden zijn:

- Er wordt gebruik gemaakt van een VPN om de IP adressen niet te kunnen vinden, als er wordt binnengedrongen. De verbinding tussen de client en server is moeilijker binnen te dringen doordat er een firewall aanwezig is die de verbindingen tussen de server en de client voortdurend monitort.
- Door SSH de gebruiken bij een verbinding krijg je een beschermde verbinden en wordt alle data geincrypt.
- Er worden bepaalde wachtwoordvereisten gemaakt zodat de wachtwoord niet makkelijk te kraken valt.
- Kijk welke poorten, protocollen en services er op de server worden gedraaid. Op die manier weet je waar je mogelijke aanvallen kan verwachten zodat je het kan voorkomen.

Data flow diagram