ADVIESRAPPORT

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

Onderzoeksvragen

Voor het adviesrapport hebben wij per categorie een aantal vragen opgesteld. Aan de hand van deze vragen wordt er een advies gegeven op het beveiligingsrapport.

Design

- Is de constructie van de bank stevig genoeg en gaat het niet makkelijk uit elkaar of stuk?
- Is het geld moeilijk bereikbaar en geïsoleerd zodat diefstal wordt voorkomen?
- Is het uitgifte van het geld zodanig geconstrueerd dat het geld nooit wordt blootgelegd aan de gebruiker en alleen de gevraagde bedrag?
- Wordt er gekeken in het geval dat er wel een diefstal of vernieling is, hoe er vastgelegd kan worden wie de daar is.

User interface

- Is bij het intoetsen van de pincode de cijfers verborgen door bijv. sterretjes waardoor er door iemand anders de pincode niet kan worden gezien?
- Wordt de sessie gesloten wanneer de gebruiker de sessie afbreekt of de sessie afrondt?
- Wordt het pasje eerst teruggegeven voordat de gebruiker het geld krijgt, zodat de pasje niet per ongeluk wordt vergeten omdat het geld eerst wordt gegeven?
- Is het niet mogelijk om meer te pinnen dan dat de gebruiker beschikbaar heeft of meer dan wat het geldautomaat beschikt

Database

- Zijn de accounts die toegang hebben tot de database goed beveiligd met een sterke wachtwoord?
- Wordt het pasje geblokkeerd als de gebruiker de code te vaak fout invoert en op het moment dat de gebruiker het correct invoert wordt de teller weer gereset?
- Zijn de pincode zodanig beveiligd dat het niet mogelijk is om de pincodes te zien is in het database?
- Kan de pinpas op aanvraag worden geblokkeerd zodat er geen verdere misbruik ermee kan worden gemaakt indien het wordt gesloten.

Server

- Is de connectie van de user interface naar de server goed beveiligd zodat het niet onderschept kan worden door iemand die eer misbruik van wilt maken?
- Is de connectie van de beheerder naar de server goed beveiligd zodat er geen misbruik van gemaakt kan worden?
- Is de server zelf goed beveiligd en wordt het goed gemonitord zodat een potentiële aanvaller kan worden gedetecteerd en vervolgens geblokkeerd?
- Zijn de gebruik van de services en poorten van de server bekend en zijn de onnodige services en poorten gedeactiveerd zodat de mogelijke aanval punten bekend zijn?

Beveiligingsadvies

Aan de hand van de onderzoeksvragen van de beveiligingsrapport is het volgende beveiligingsadvies opgesteld.

Design

- Er wordt aangegeven dat het design van het geldautomaat robuust wordt, maar verder wordt er niet op ingegaan op welke manier het robuust wordt en welke materialen en wordt gebruikt om het robuust te maken. Het advies is om een duidelijke omschrijving te geven en duidelijke materiaal keuzes erbij te vermelden. Natuurlijk moet er ook gekeken worden naar de beperkingen die er zijn en dat er niet een brede keuze is aan materialen.
- Er wordt aangeven dat het geldautomaat niet zomaar geld beschikbaar stelt als het wordt omgestoten. Er is geen omschrijving wat voor maatregel er wordt genomen hoe het geld in zo'n geval wordt beveiligd, doordat bijvoorbeeld de plek waar het geld kan uitkomen wordt gesloten met behulp van een evenwichtssensor die aangeeft dat het geldautomaat uit balans is.
- Er wordt niet omschreven bij mogelijke vernieling of er een bepaalde systeem is om vast te leggen wie mogelijke de dader kan zijn, door bijvoorbeeld een camera te installeren in het geldautomaat.

User interface

- Er is niet terug te vinden hoe de pincode beveiligd wordt op het moment dat het in de user interface wordt ingetoetst door bijvoorbeeld het weer te geven als sterretjes. Zo verklein je de mogelijkheid dat een persoon de pincode te zien krijgt en op misbruik van de pasje van een gebruiker.
- Er wordt niet gekeken naar de saldo van de gebruiker dus de gebruiker kan mogelijk een bedrag invoeren doe hoger is dan de saldo die zij hebben. Er moet in de user interface een melding worden gegeven als de gebruiker een bedrag wilt pinnen die hoger is dan het bedrag die de gebruiker op zijn bankrekening heeft.

Database

- Er wordt niet aangegeven of de accounts beveiligd gaan worden en hoe ze het gaan beveiliging. Dit kan door alle accounts die toegang hebben tot de database een sterke wachtwoord te geven die voldoen aan een bepaalde standaard. Voor meer info over sterke wachtwoorden klik hier.
- Verder wordt er aangegeven dat de data wordt geencrypt maar er wordt niet op ingegaan op welke manier het geincrypt wordt. Er kan bijvoorbeeld gekozen worden om een AES encryptie toe te passen. Voor meer info over database encryptie klik hier.
- Ook wordt er niet aangegeven of de pincode in de database zelf worden gehashed zodat het niet zichtbaar wordt voor de beheerders van de database. Het is altijd belangrijk dat er niet bij de pincodes kan komen of de pincodes kan zien zodat de beveiliging van de gebruikers wordt gewaarborgd.

Server

- Er wordt niet aangegeven hoe de beveiliging van de data uitwisseling tussen de user interface en server gebeurt. Dit kan gebeuren door middel van een VPN verbinding.
- Verder wordt er niet aangegeven hoe de server zelf beveiligd gaat worden. Een van de stappen die genomen kunnen worden om je server te beveiligen is het hebben van een firewall. Die zorgt ervoor dat de activiteiten die plaats vinden op de server en de verbindingen er naar toe worden gemonitord. Voor meer info over een beveiligde server klik hier.
- Ook wordt er niet aangegeven hoe de connectie tussen de beheerder en de server wordt beveiligd wanneer de beheerder op de server iets wilt uitvoeren. Een van de meest gebruikte beveiliging is SSH voor het verbinden naar de server. Voor meer info over het verbinden via een SSH tunnel klik hier.
- Er wordt niet aangegeven hoe services en poorten van de server worden bijgehouden en gecontroleerd. Het is belangrijk om te weten wat voor services en poorten er worden gebruikt en welke er niet worden gebruikt zodat de on gebruikte uitgeschakeld kunne worden. Zo zijn er minder aspecten die je moet beveiligen en waar een hacker kan misbruiken.

Advies landsbank

Het landsbank of hoe wij het ook noemen de centrale bank is de bank die zorgt voor alle communicatie tussen alle banken in het land. Er zijn bepaalde eisen verbonden om je aan te sluiten aan het landsbank. De eisen worden beschreven in het document SCB_document, die wordt toegevoegd als bijlage.

Elke landsbank heeft een land code, dat is de code van de herkomst van de landsbank. Die land code wordt ook gebruikt in het IBAN nummer de elke bank gebruikt zodat je kan herkennen van welke land een bepaalde bank is.

Verder heeft elke bank een IBAN nummer die voldoet aan de algemene IBAN regels en structuur, om te zien wat dat zijn klik hier. Iedere bank die aangesloten is aan het landsbank die moet voldoen aan deze samenstelling van het IBAN nummer.

Vervolgens moet de landsbank de communicatie structuur van elke bank zien te weten van elke bank en die weer converteren naar de communicatie structuur van de andere bank zodat er mogelijke botsingen tussen gegevens voorkomen kan worden.

Elke bank moet het CA certificaat hebben waarbij er een publieke en private key is. De publieke key wordt gegeven aan de verschillende banken zodat de gegevens beveiligd worden verstuurd en alleen de bank die het moet ontvangen het kan openen.

De bijdrage dat we kunnen leveren aan de landsbank is een bepaalde structuur van het verzenden van informatie zodat op juiste manier worden ontvangen en verwerkt en zo ook op de juiste manier gedeeld kunnen worden.

Bijlage: SCB_document