**Beveiligingsplan Groep 6 Project 3/4**



Door: Maarten Brilleman: 0984801,

Gillbert Resida: 0990026,

Rob Wolters: 0993362,

Eki Pratama: 0989818

# **Inhoudsopgave**

Inhoud

[**Inhoudsopgave** 1](#_Toc35791762)

[**Deelvraag 1: Hoe beveiligen wij het fysieke gedeelte van het gelduitgifte systeem?** 2](#_Toc35791763)

[**Inleiding** 2](#_Toc35791764)

[**De gelduitgifte lade** 2](#_Toc35791765)

[**Vormgeving pinautomaat** 3](#_Toc35791766)

[**Deelvraag 2: Hoe beveiligen wij onze bank tegen de mens?** 4](#_Toc35791767)

[**Inleiding** 4](#_Toc35791768)

[**Fraude** 4](#_Toc35791769)

[**Diefstal** 4](#_Toc35791770)

[**Deelvraag 3: Hoe zorgen we ervoor dat de database veilig blijft?** 5](#_Toc35791771)

[Literatuurlijst 6](#_Toc35791772)

**Hoofdvraag: Wat zijn de noodzakelijke maatregelen die getroffen moeten worden om onze bank te beschermen?**

Als bank krijgen wij te maken met verscheidene veiligheidsrisico’s voor onze assets. Onder deze assets scharen wij onder andere alle gegevens die wij in onze database hebben staan, de toegepaste hardware in de bankautomaat waarop het besturingssysteem geladen is alsmede het fysieke geld dat aanwezig is in onze geldautomaat.

Vanwege de hele verschillende eigenschappen van deze assets en de hele verschillende manier van opslag, komen er hele verschillende manieren van beveiliging bij kijken. Bij de fysieke bescherming van de bankautomaat moet rekening gehouden worden in het ontwerp van de behuizing. Zorgen dat cruciale onderdelen niet van buitenaf toegankelijk zijn en dat de bankautomaat dermate robuust is dat deze tegen een stootje kan en niet gelijk zijn inhoud weggeeft.

Het software gedeelte leunt meer op nieuwerwetse beveiligingstechnieken. Maatregelen die hier toegepast kunnen worden zijn technieken zoals data-encryptie, wachtwoord versleuteling, verscheidene niveaus aan autorisatie en meerdere lagen van authenticatie.

Met dit in het achterhoofd willen wij, door middel van het beantwoorden van 3 deelvragen, een antwoord zoeken op de hoofdvraag: Wat zijn de noodzakelijke maatregelen die getroffen moeten worden om onze bank te beschermen?

# **Deelvraag 1: Hoe beveiligen wij het fysieke gedeelte van het gelduitgifte systeem?**

## **Inleiding**

De voornaamste functie van een pinautomaat is het verkrijgen van geld. Dit is ook wat de pinautomaat een doelwit maakt voor criminelen. De fysieke beveiliging van een pinautomaat is daarom uiterst belangrijk. Om niet alleen het geld binnen in de automaat te beschermen, maar ook onze reputatie en klandizie. Niemand wil immers pinnen bij een onbeveiligde pinautomaat.

## **De gelduitgifte lade**

De gelduitgifte lade is het zwakste punt van de pinautomaat. De lade opent om het gepinde geld aan de klant te geven, maar kan hierdoor ook toegang binnen ons systeem geven aan criminelen of ongewenst gespuis. Het is daarom ook van groot belang dat wij dit onderdeel van de pinautomaat voldoende beveiligen tegen binnendringers, maar daardoor onze klanten niet teveel hinderen met onze getroffen maatregelen.

Wanneer dit onderdeel niet voldoende beveiligd is geven wij indringers ongelimiteerd toegang tot alle kritieke systemen: Het gelduitgifte systeem, de microcontrollers en aanwezige computersystemen en de gebruikersinterface.   
  
De beveiliging van de gelduitgifte lade is daarom het meest kritiek en vereist het meeste aandacht en de beste beveiliging.  
  
Eén van de getroffen maatregelen is het plaatsen van een schot binnen in de pinautomaat, om zo de handen of gereedschap van binnendringers te hinderen. Zonder de uit te geven biljetten te blokkeren.  
Een andere getroffen beveiliging is het plaatsen van printerrollen. Deze rollen zijn geplaatst tussen de geldhouderbakjes en de gelduitgifte lade. De rollen zullen draaien, na een signaal van het systeem, wanneer er geld klaar ligt om uitgegeven te worden zodat het systeem ze netjes de geldlade in duwt. De rollen zullen, net als het geplaatste schot, handen of gereedschap van binnendringers hinderen en blokkeren.

## **Vormgeving pinautomaat**

De behuizing en vormgeving van het omhulsel rondom de pinautomaat is onze eerste laag van bescherming tegen dieven en hackers. Dit is ook het eerste wat een dief zal zien en zal het onderwerp zijn van de eerste pogingen om de pinautomaat binnen te dringen. Eventuele gaten of onbeheerde toegangspunten zijn onacceptabel en moeten daarom met grote zorg vermeden worden en beveiligd worden.

Omdat na het implementeren van de pinautomaat nog onderhoud plaats moet vinden, en over tijd het geld bijgevuld dient te worden is constante toegang tot de pinautomaat vereist. En moet de toegang daarom groot genoeg zijn om onderhoud en constante bevoorrading van het geld mogelijk te maken.   
Dit onderdeel introduceert ook een zwakte binnen het systeem. Waar wij ons goed tegen dienen te beveiligen.   
  
Aangezien een open luik die toegang geeft tot de gehele pinautomaat voor monteurs, ook een toegangspunt kan zijn voor dieven en indringers heeft het een groot risico.   
Maar aangezien dieven en indringers geen grof gereedschap of zware explosies zullen gebruiken is deze beveiliging niet zo kritiek als dat van de geldlade.   
  
Een algeheel afsluitend omhulsel rondom het gelduitgifte systeem zal voldoende zijn om het systeem tegen onze doelgroep te beschermen. Een luik op de achterkant met een standaard hangslot zal voldoende toegang geven aan werknemers, en inbrekers buiten houden.

# **Deelvraag 2: Hoe beveiligen wij onze bank tegen de mens?**

## **Inleiding**

Als we aan een pinautomaat denken hebben het vaak over geld pinnen. Het is een van de meest bekende processen die voor een gebruiker gebeuren bij een bank, maar het is ook vaak een van de meest kwetsbare processen aangezien je in het openbaar je geldzaken aan het regelen bent die normaliter privé horen te blijven. Om deze reden is het ook een aantrekkelijk process voor criminelen die het geld van andere willen bemachtigen. Dit doen ze vaak door fraude, misbruik of diefstal te plegen. Daarom hebben we in dit beveiligingsrapport een opstel gemaakt van hoe we hier ons en onze klanten kunnen beveiligen.

## **Fraude**

Een van de meest voorkomen manier om de bank en gebruikers aan te vallen is via fraude. Criminelen zijn tegenwoordig heel creatief en inventief om wegen te vinden naar de gebruikers hun bankgegevens. Hierbij komt fraude erg vaak aan bod. Een techniek die met fraude te maken heeft en vaak wordt gebruikt door criminelen is phishing. Bij phishing doen de criminelen net alsof ze bij de bank horen en sturen dan verdachte mails door naar de gebruikers. Daarom is het van belang dat we onze gebruikers hulpmiddelen en guidelines aanbieden zodat ze zich als het ware kunnen beveiligen tegen dit soort aanvallen. Als we dit niet doen dan lopen erg veel gebruikers gevaar vanwege onwetendheid. De beveiliging tegen fraude is daarom ook een van de belangrijkste aandachtspunten om de bank te beveiligen.

## **Diefstal**

Een ander veel voorkomend gevaar is diefstal. Diefstal is voornamelijk het grootste gevaar bij het pin proces want vaak wordt het gepleegd d.m.v geweld. Het komt vaak voor dat criminelen de passen van gebruikers stelen om vervolgens een transactie met de pas te doen. Daarom is het van belang dat onze gebruikers hun pas kunnen blokkeren als hij gestolen wordt of dat de pas automatisch blokkeert als de pincode meer dan drie keer fout wordt ingetoetst. Als extra beveiliging kan de pas alleen gedeblokkeerd worden als de gebruiker de bank belt en aan kan tonen dat hij of zij eigenaar van het account is. Om fraude hierbij te voorkomen worden er een aantal vragen gesteld die alleen de gebruiker weet en niemand anders, dit zorgt weer voor een extra beveiliging laag. De beveiliging tegen diefstal is daarom een van de belangrijkste aandachtspunten om ervoor te zorgen dat de bank beveiligd is.

**Misbruik**

Maar criminelen van buitenaf zijn niet het enige gevaar voor onze bank. Hoewel we hopen dat dit nooit het geval zal zijn bij onze eigen bank gebeurt het nog al te vaak dat de werknemers misbruik maken van de rechten die ze hebben door hun functie. Een van de getroffen maatregelen is daarom dat wij ervoor gaan zorgen dat elke medewerker de juiste hoeveelheid rechten heeft en zo gemonitord kan worden. Als we dit niet doen maken we het onszelf erg moeilijk en lopen onnodig gevaar als onbevoegde bij bepaalde data kunnen komen in de database van de bank.

# **Deelvraag 3: Hoe zorgen we ervoor dat de database veilig blijft?**

Alle informatie betreft de bank is opgeslagen in de database. Het is van groot belang om dit dan ook zo goed mogelijk te beschermen. Bovendien gaat alle communicatie indirect naar de database toe.

Wanneer een klant wil pinnen, maakt de ATM verbinding met de php server die dan vervolgens weer verbinding gaat maken met de server waar de database is opgeslagen. De database stuurt de gevraagde informatie vervolgens op.

Wanneer een medewerker een update aan de database wilt uitvoeren, heeft de medewerker direct toegang tot de php server. Via de php server wordt er een update op de database uitgevoerd.

Wanneer een klant wil pinnen bij een andere bank, geld precies hetzelfde als bij het pinnen bij de eigen bank, alleen wordt er eerst verbinding gemaakt met de N.O.O.B. server. De ATM van de desbetreffende bank maakt een verbinding met de N.O.O.B. server van school die vervolgens een verbinding maakt met de php server.

Om de veiligheid van de database te waarborgen, is er gekozen om via een php server te verbinden. Die maatregel is genomen om zorg te dragen dat de verbinding naar de database toe niet direct plaatsvindt. Zo zijn bijvoorbeeld de gegevens van de database nog steeds veilig wanneer iemand direct toegang heeft tot de php server.

Ook willen we ervoor zorgen dat de verbinding tussen de cliënt en de database veilig blijft. Om dit veiliger te krijgen, gaan we bij de datacommunicatie gebruik maken van het SSL-protocol. Dit protocol zorgt ervoor dat de data-verbinding versleuteld verstuurd wordt. Op het moment dat de data wordt onderschept moet deze eerst gekraakt worden voordat het leesbaar wordt. Verder willen we gevoelige informatie in de database extra beveiligen. Zo gaan we deze informatie hashen om ervoor te zorgen dat deze extra veilig wordt.

De zwakte in deze toepassing is dat alle gehashte informatie alsnog achterhaald kan worden. Met de zogeheten brute force attack worden alle mogelijke combinaties uitgeprobeerd om aan de data te komen. Dit hoeft niet per se een probleem te zijn omdat dit heel veel tijd kan kosten, het kan zelfs jaren duren voordat dit wordt achterhaald. Om dit toch nog extra te beveiligen gaan we de gegevens zoals wachtwoord regelmatig veranderen. Dit geeft steeds een andere hash wat ervoor zorgt dat het kraken nog moeilijker wordt.

# Literatuurlijst

G. Rajendran, R. S. Ragul Nivash, P. P. Parthy and S. Balamurugan, "Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures," 2019 International Carnahan Conference on Security Technology (ICCST), CHENNAI, India, 2019, pp. 1-6.

Valade, J. (2007). *PHP and MySQL For Dummies: Vol. 3rd ed*. For Dummies.

S. Pasandideh, L. Gomes and P. Maló, "Improving Attack Trees Analysis using Petri Net modeling of Cyber-Attacks," 2019 IEEE 28th International Symposium on Industrial Electronics (ISIE), Vancouver, BC, Canada, 2019, pp. 1644-1649.

D. Mitropoulos, P. Louridas, M. Polychronakis and A. D. Keromytis, "Defending Against Web Application Attacks: Approaches, Challenges and Implications," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 2, pp. 188-203, 1 March-April 2019.







