|  |  |
| --- | --- |
| Beveiligings- adviesrapport  Project 3/4 | Abstract  [Trek de aandacht van uw lezer met een veelzeggend citaat uit het document of gebruik deze ruimte om een belangrijk punt te benadrukken. Sleep dit tekstvak als u het ergens anders op de pagina wilt plaatsen.]  Jia-jie Yeh (0992427)  [Cursustitel] |

Inhoudsopgave

[Hst 1. Beveiliging rapport 2](#_Toc70606801)

[1.1 Data Flow Diagram (DFD) 2](#_Toc70606802)

[1.2 Risicoanalyse 3](#_Toc70606803)

[1.3 Maatregelen 3](#_Toc70606804)

[1.4 Attack tree 4](#_Toc70606805)

[Literatuurlijst 5](#_Toc70606806)

[Hst 2. Advies rapport 6](#_Toc70606807)

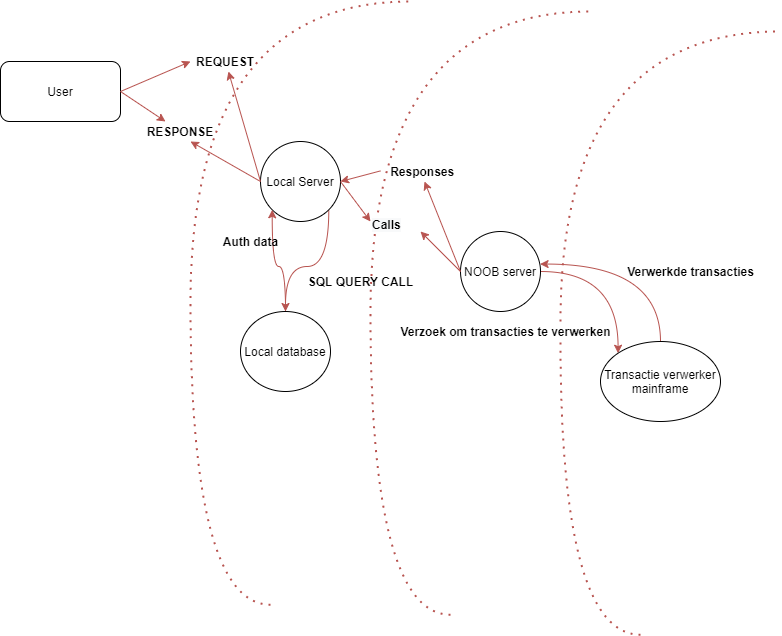
[2.1 onderzoeksvragen 6](#_Toc70606808)

[2.2 beveiligingsadvies 6](#_Toc70606809)

[2.3 Advies landbank 6](#_Toc70606810)

# Hst 1. Beveiliging rapport

## Data Flow Diagram (DFD)



## Risicoanalyse

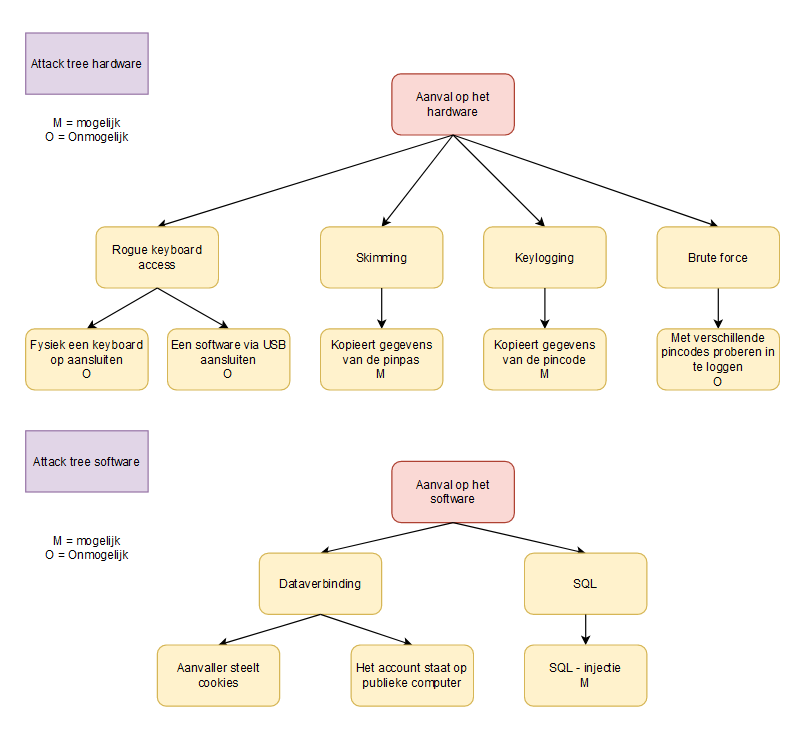
|  |  |  |
| --- | --- | --- |
|  | Soorten risico aanvallen | Uitvoering |
| 1 | Rogue keyboard access | Dit is een fysiek toetsenbord koppelen aan een pinautomaat en vervolgens een stukje code of een SQL – injectie executeren. De aanvaller kan de pinautomaat dan controleren. |
| 2 | Skimming | Met deze methode dupliceer je de gegevens van een pinpas. Dit gebeurd door een replica te maken van een pinautomaat en dat plaatsen ze aanvallers op het pin sectie. |
| 3 | Keylogging | Dit is het zelfde geval van skimming, maar dan voor de gebruiker zijn pincode. Er wordt dan een replica keypad over het standaard pin keypad gelegd, waardoor de gebruiker zijn pincode wordt gestolen. |
| 4 | Dataverbinding | Als er iemand tussen de dataverbinding van het systeem komt, dan is het systeem is niet versleuteld. Hierdoor zijn de onderdelen bijvoorbeeld; de informatie van de keypad en de gui zeer gevoelig. |
| 5 | SQL | De gui moet beveiligd worden voor aanvallen, zoals SQL-injectie. Hierdoor krijgt de aanvaller gebruik tot je data in je database. Dit kan vernietigd of gestolen worden. |
| 6 | Brute force | De aanvaller kan ook via brute force aanvallen op meerdere onderdelen van het systeem. Hierbij kunnen de data zoals; pincodes en wachtwoorden van de gebruiker te verkrijgen. |

## 1.3 Maatregelen

|  |  |  |
| --- | --- | --- |
|  | Soorten risico aanvallen | Oplossingen |
| 1 | Rogue keyboard access | Dit is een van de makkelijkste aanvalssoort op de ATM, waardoor het ook gelijk makkelijk te detecteren is. Hierdoor kan je als een nieuw apparaat wordt toegevoegd dan wordt het ATM stop gezet. Je kan ook speciale karakters accepteren. |
| 2 | Skimming | Dit kan je oplossen om door een elektromagnetische puls. Dit geeft een korte schok aan de skimmer. De schok verstoort of beschadigd de skimmer. |
| 3 | Keylogging | De aanvaller is moeilijk te detecteren, want tegenwoordig niet altijd een keypad replica gebruikt, maar ook een USB-stick. Eerst was de oplossing voelen aan de toetsenbord en kijken of het nep is. Dit is het zelfde geval bij het gebruik van de rogue keyboard. |
| 4 | Dataverbinding | Dit valt op te lossen om beveiliging te maken door middel van SHA-3^15 hash of encryptie. Hierdoor krijgt de aanvaller onleesbare data. |
| 5 | SQL | Deze aanval kan je voorkomen om de input validatie te gebruiken. |
| 6 | Brute force | Om het systeem te beschermen tegen DDoS aanvallen van de aanvaller kan je bijvoorbeeld een Anti DDoS systeem gebruiken. In Nederland is een bekende zogenaamd NaWas. Er is ook een Nationale Anti-DDoS coalitie. |

## 1.4 Attack tree

Om een helder beeld te krijgen van een beveiligingssysteem wordt er een attack tree gemaakt. Deze attack tree geeft een beeld over de situaties van de risico aanvallen op het systeem en hoe het systeem op reageert.



## Literatuurlijst

Beveiligingsbronnen

1. <https://www.kaspersky.com/blog/atm-attacks-2/15160/>

<https://jarnobaselier.nl/rogue-access-point-easy-wifi-hacking/>

1. <https://www.lookingglasscyber.com/blog/atm-hacking-you-dont-have-to-pay-to-play/>

<https://www.tpsworldwide.com/atm-skimming-preventing-bank-card-hacks/>

<https://mens-en-samenleving.infonu.nl/diversen/22626-hoe-skimmers-skimmen.html>

1. <https://www.pandasecurity.com/en/mediacenter/security/keyloggers-be-careful-what-you-type/>

<https://ecobank.com/personal-banking/security-centre/scams/keyloggers>

<https://www.malwarebytes.com/keylogger/>

1. <https://www.vpngids.nl/veilig-internet/surfen/wat-is-encryptie/>
2. <https://kinsta.com/nl/blog/sql-injecties/>

<https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html>

1. <https://www.ncsc.nl/onderwerpen/ddos/het-nederlandse-anti-ddos-initiatief>

<https://www.nbip.nl/nawas/>

# Hst 2. Advies rapport

## 2.1 onderzoeksvragen

* Is het ontwerp compleet, of mist het nog informatie?

Nee, het mist geen informatie en ziet er compleet uit. Het bevat alle standpunten en bij de literatuurlijst zijn alle belangrijke bronnen vermeld en door een website link verbonden.

* Kan er iets kapot gaan en verbeterd worden?

* Zie je nog blinden vlekken die de peergroep gemist heeft?
* Zijn de maatregelingen sterk genoeg?
* Zijn de informatiebronnen uitgebreid genoeg?

De literatuurlijst is goed uitgebreid en verwerkt de standpunten van de bronnen die gebruikt zijn. Dit geeft een goed zicht waar het informatie vandaan komt.

* Ziet de attack tree van de peergroep goed uit?

De attack tree van de peergroep is ook in 2 delen verdeeld. In een hardware -en software gedeelte. Het hardware gedeelte is verdeeld hoe het fysiek ingebroken wordt, hoe moeilijk de hardware componenten betast worden en hoe de bank bescherming van de gelddispenser. Het software gedeelte is verdeeld in database hacken, datastroom onderscheppen, de GUI en pinpas stelen. Hier worden de moeilijkheidsgraden van de aanvallen gemankeerd met een ‘P van possible’ en ‘I van impossible’. Dit zorgt ervoor een gedetailleerde overzicht over de aanvallen op de bank.

* Is de DFD compleet?

Alle standpunten van de bank zijn er in verwerkt. De gebruiker heeft dan een laag voor het invoeren van zijn data dus de pincode, balans en card ID. Dit wordt dan verstuurd naar de volgende laag en dat is de ATM laag. Hier wordt de data van de gebruiker verstuurd naar de landelijke server. Dit wordt dan vergeleken met de banken die er allemaal verbonden zijn aan de landelijke server via een Iban id. Anders gaat het via de Noob server als het uit een andere land komt. Hier wordt dan de data terug gestuurd.

## 2.2 beveiligingsadvies

## 2.3 Advies landbank