23-3-2020

Gemaakt door: Jelle Beek (0994034), Tessa Paalvast (0989691), Ziwe Zhang (0984223) en Joshua Asmowidjojo (0991620)

Hogeschool rotterdam cmi ti1d

Batbank

Beveiligingsrappoort

Inleiding

De batbank is één van de topbanken van America. Deze moet natuurlijk goed beveiligd zijn. Om een goede beveiliging te hebben, moeten we eerst een inzicht krijgen op de kwetsbaarheden en de mogelijke aanvallen bij onze bank. In dit verslag gaan we hierop in en zullen we op basis van onze bevindingen de bank beveiligen.

Hoofd- en deelvragen

Onze hoofdvraag in dit verslag is:

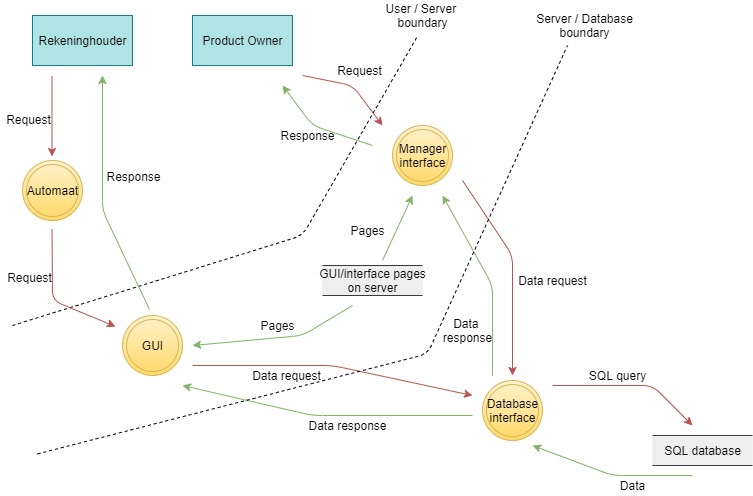
* Hoe beveiligen wij onze bank zo goed mogelijk?

Om deze vraag te beantwoorden, zullen we de volgende deelvragen gebruiken:

* Wat wil ik beschermen?
* Wie zijn mogelijke aanvallers bij een bank?
* Wat zijn de mogelijke aanvallen bij een bank?
* Hoe beveiligen we onze bank tegen deze aanvallen?

Bankstructuur

DFD

Om alle dreigingen van onze bank te kunnen vinden is het handig om een schets te hebben van hoe de bank werkt. Hiervoor hebben wij een DFD (data flow diagram) gemaakt.

Je kan zien dat er maar twee users zijn bij de bank. Er moet in ieder geval gezorgd worden dat ons systeem deze users goed kan identificeren. De managerinterface is waarschijnlijk één van de belangrijkste dingen om te beschermen. Hier zullen veel mensen proberen in te breken, omdat je hier natuurlijk veel meer kan dan de gemiddelde gebruiker. Dit sluit niet buiten dat de GUI niet aangevallen zal worden.

Dreigingen

Potentiële aanvallers (adversaries)

Voor een goed inzicht in de aanvallen zullen we eerst mogelijke aanvallers in kaart brengen. Iedereen zou een aanvaller kunnen zijn, zo kan de manager van de bank aanvallen. Ook kunnen de systeem admins van de hoofdbank (NOOB) ons proberen aan te vallen.

Vaak zijn de aanvallers niet betrokken bij de bank. Deze mensen kunnen hackers zijn, maar ook dieven.

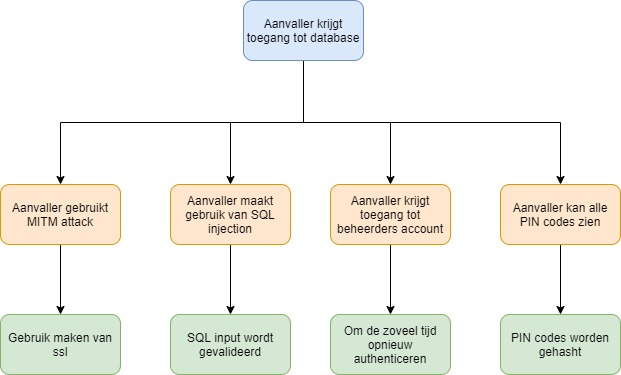
Potentiële doelwitten (assets)

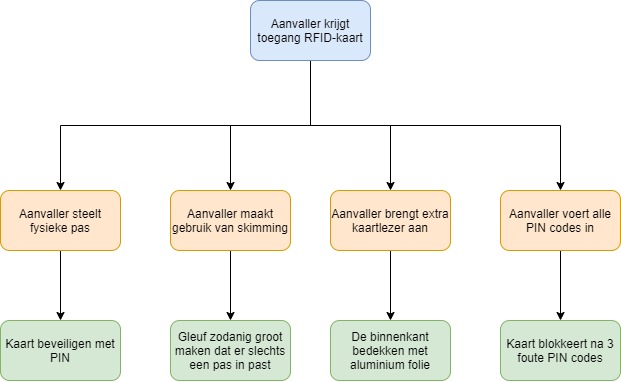
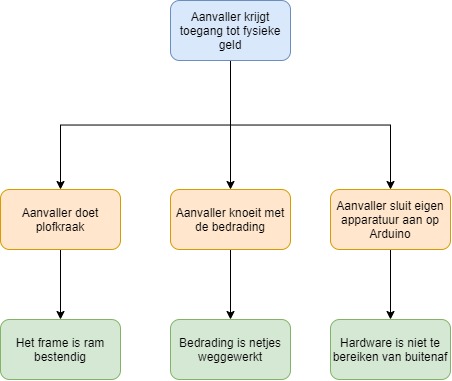
Ook is het handig om te weten wat we willen beschermen. Onze bank heeft een aantal punten die wij moeten beschermen. Één van de belangrijkste assets bij ons is de database. Als iemand hier toegang tot krijgt kan hij zichzelf heel veel geld geven of stelen van anderen.

Een andere asset is het geld in de gelddispenser, wij willen natuurlijk niet dat je zomaar bij al het geld kan. Ook de managerinterface is een asset die wij goed moeten beschermen.

Potentiële aanvallen

Door de adversaries en assets te combineren kunnen wij een aantal mogelijke aanvallen schetsen. Hieruit komen de volgende attack trees, waarbij ook gelijk oplossingen voor deze aanvallen staan.

Bij de eerste attack tree staan de mogelijke aanvallen van een hacker.

Bij de volgende attack tree staat de RFID-kaart (pinpas) centraal.

De laatste attack tree gaat over het gebruik van fysiek geweld om geld te krijgen.

Beveiliging

De manieren om een bank te beveiligen staan eigenlijk al in de attack trees, maar we gaan hier dieper op de mogelijke methodes in.

Database

Om een database te beveiligen moet alle software up-to-date zijn. Ook is het handig om te zorgen dat alle functies die niet nodig zijn, uitgeschakeld zijn. Dit geldt ook voor de rechten van de personen die toegang tot de database hebben. Het is handig om alsnog alle activiteit van de database in de gaten te houden.

Voor het beveiligen tegen sql injection zijn er een aantal verschillende manieren. Je kunt bijvoorbeeld zorgen dat er niks wordt uitgevoerd als er speciale tekens worden aangetroffen die een typerend zijn voor sql injection. Dit zijn tekens zoals ‘, “ of = of zelfs het woord ‘UNION’. Een andere manier is om ‘prepared statements’ te gebruiken. Je kunt ook de input valideren d.m.v. plugins of addons.

Persoonlijke gegevens

Voor de persoonlijke gegevens van een gebruiker gebruiken wij encryptie. Hierbij gebruik je een ‘sleutel’ om de gegevens onbruikbaar te maken voor personen die deze sleutel niet hebben. Dit wordt ook gebruikt in ssl waardoor je een MITM (Man In The Middle) aanval kan vermijden.

Bij een wachtwoord of de pincode van een gebruiker is het niet handig om encryptie te gebruiken. Hiervoor kan je hashing gebruiken. In tegenstelling tot encryptie kan je na het hashen niet terugkomen op het wachtwoord. Bij hashing wordt elk ingevoerd wachtwoord ook gehasht en dit wordt vergeleken met de hash van het goede wachtwoord.

Accountbescherming

Om accounts te beschermen kan je verschillende dingen doen. Om te beginnen kan je ervoor zorgen dat gebruikers TFA (Two factor Authentication) moeten gebruiken, zodat je met alleen het wachtwoord niet veel kan. Ook kan je ervoor zorgen dat een gebruiker elke maand zijn wachtwoord/pincode moet wijzigen. Dit is echter niet reëel.

Als een gebruiker of bijvoorbeeld de manager ingelogd staat en wegloopt is er natuurlijk een risico dat iemand hier misbruik van maakt. Om dit te voorkomen kan je bijvoorbeeld zorgen dat er om een bepaald aantal minuten uitgelogd wordt.

Fysieke aanvallen

Om te zorgen dat je niet zomaar geld kan pakken of het apparaat slopen moet je zorgen dat de ATM een sterk frame heeft. Ook moet er gezorgd worden dat er geen draden of hardware zichtbaar is, als dit wel het geval is kan er misbruik van gemaakt worden.

Als extra maatregel kan je ook nog zorgen dat er sensoren op de ATM zitten die meten of er geknoeid mee wordt om vervolgens de biljetten ongeldig te maken zoals met verf.

Er zouden ook camera’s geïnstalleerd worden die kunnen zien of iemand met de ATM knoeit. Dit is ook handig om te kunnen kijken of er externe apparatuur op de ATM wordt geïnstalleerd die een pas kunnen klonen of een camera die de pincode registreert. Ook is het handig om af en toe een inspectie te doen op de bank om voor deze extra apparaten te controleren.

Conclusie

Om te zorgen dat onze bank goed beveiligd is gaan we een aantal maatregelen nemen.

Wij zullen bij de communicatie met de database zorgen dat er geen sql injection mogelijk is door ‘prepared statements’ te gebruiken, we zullen ook de input valideren. Alle persoonlijke gegevens zullen wij encrypten of hashen.

In het geval dat een aanvaller in het beheerders account komt, zorgen we ervoor dat dit account zich om de zoveel tijd opnieuw moet authentiseren, hier zullen we ook zorgen dat je meer moet invullen dan 1 wachtwoord.

Om een fysieke aanval tegen te gaan zullen we onze ATM sterk maken en zorgen dat je van buitenaf niet bij de hardware komt. De RFID-reader krijgt maar een heel klein gat zodat die net de pas kan scannen. Hierdoor voorkomen wij dat er externe apparatuur wordt geïnstalleerd om passen te kunnen klonen.

Bronnen

<https://www.esecurityplanet.com/network-security/6-database-security-best-practices.html>

<https://www.hacksplaining.com/prevention/sql-injection>

Databases beveiliging

<https://www.byte.nl/kennisbank/onderhoud/gegevens-beveiligen-met-encryptie-en-hashing>

Encryptie

<https://www.bankinfosecurity.com/10-tips-to-improve-atm-security-a-2852>

Bank beveiliging

[https://mods-n-hacks.gadgethacks.com/how-to/block-rfid-signals-build-rfid-reader-detector-and-make-custom-rfid-tags-0138673](https://mods-n-hacks.gadgethacks.com/how-to/block-rfid-signals-build-rfid-reader-detector-and-make-custom-rfid-tags-0138673/)

Skimming

<https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc785811(v=ws.10)?redirectedfrom=MSDN>

SSL

<https://owasp.org/https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc785811(v=ws.10)?redirectedfrom=MSDN-community/attacks/Man-in-the-middle_attack>

MITM aanval