Adviesrapport

Groep 4 advies voor groep 3

Chen Yen Wang | 0988936
Storm Hoogstrate | 0984053
Tala Hammed | 0995285
Pim van den Toorn | 0984004

Inhoudsopgave

Review beveiligingsplan & bijbehorende adviezen

De Hogeschool Rotterdam heeft ons gevraagd om een adviesrapport te schrijven over het beveiligingsplan wat zij aan ons hebben voorgedragen. Om dit adviesrapport gericht te kunnen opstellen gaan wij hierin de volgende vragen beantwoorden:

- Voldoet het plan aan de eisen van een plan?
- Zijn er nog andere bedreigingen die dit beveiligingsplan mist?
- Zijn de maatregelen die dit beveiligingsplan bevat realistisch?

Hieronder zullen wij deze vragen beantwoorden en onderbouwen met argumenten en/of bronnen.

Voldoet het plan aan de eisen van een plan?

Het verslag heeft een Data Flow Diagram, alleen wordt hier geen uitleg bij gegeven wat er gebeurt in deze diagram en waarom dit is opgesteld. De lezer zal zo'n diagram niet makkelijk kunnen begrijpen zonder dat hem uitgelegd wordt wat dit diagram inhoudt. Ons advies hiervoor is dus om elk (ingewikkeld) schema, diagram en tabel te voorzien van een stukje uitleg.

Ten slotte hebben wij nog een advies over een aantal andere onderdelen wie wij missen in het beveiligingsrapport, bijv. hoe de hardware en de database wordt beveiligd. Er wordt gesproken over van welk materiaal de behuizing van de pinautomaat om het zo robuust mogelijk te maken, maar niet over andere manieren hoe er geld kan worden gestolen via de hardware in de pinautomaat. Wij hadden graag willen zien hoe je ook andere aanvallen zou kunnen tegenhouden zoals, Man In The Middle attack (MITM).

Er wordt ook niet gesproken over de mogelijke aanvallen op de database. Met de implementatie van de AES is het wordt de database zeker veilig, maar je kan niet volledig uitsluiten dat er een aanvaller in de database kan komen. Hoe worden SQL-injecties dan tegengehouden?

Conclusie

Wij vinden dat het rapport een aantal onderdelen mist, maar voor de rest is het een netjes en verzorgd rapport.

Zijn er nog andere bedreigingen en/of beveiligingsmethodes die dit beveiligingsplan missen?

Bedreiging
Een bedreiging die niet wordt genoemd is DDoS. Hier zou minimaal een alinea aan moet woorden gewijd aangezien dit een erg veel voorkomend probleem is waarmee de banken hedendaags te kampen hebben. Ook voor de hardware zou er gekeken moeten worden naar MITM.

Beveiligingsmethodes
Een belangrijke maatregel die word gemist in dit plan met betrekking op het beveiligen van de database zijn Prepared statements die zorgen er voor dat SQL commando's niet direct in de database komen bij SQL-injecties. Ook kan er een obfuscator op de code worden gezet, op die manier is de code niet leesbaar.

Daarnaast is het hashen van bepaalde data ook een belangrijke maatregel aangezien het voor de aanvaller zeer moeilijk is om te weten wat deze data inhoudt.

Conclusie
Buiten de bovengenoemde bedreiging en beveiligingsmethodes bevat het plan alle mogelijke en nodige beveiligingsmethodes.

Zijn de beveiligingsmethodes realistisch en voldoende?
De beveiligingsmethodes die in dit verslag zijn genoemd zijn allemaal zeer realistische beveiligingsmethodes. Wel missen wij nog een aantal beveiligingsmethodes die wij erg belangrijk vinden in de beveiliging. Of jullie er bewust voor hebben gekozen om deze niet mee te nemen in het plan kan ook een reden zijn. Dat laten wij volledig aan jullie.

Communicatie binnen het land en naar de NOOB

Dit project bevat een aantal eisen. Eén van deze eisen is de communicatie tussen de banken in de klas en de andere banken in andere klassen.

Wij als projectgroep zien de communicatie als volgt uit:

Elke projectgroep moet uiteindelijk met de NOOB server communiceren. Om dit veiliger en simpeler te doen hebben we als klas afgesproken om alle groepjes eerst aan een groepsserver te koppelen en dan aan de NOOB. Deze groepsserver is de enige verbinding naar de NOOB. Alle banken in de klas dienen dan ook in verbinding te staan met de groepsserver.
Bij het ontwikkelen van deze communicatie wordt er 1 persoon vanuit elke bank naar voren geschoven voor een overleg om de 2 weken. Hierin wordt dan besproken wat er moet gebeuren om deze communicatie tussen de verschillende banken en NOOB te realiseren. Aan het eind van elke bijeenkomst worden dan ook verschillende taken verdeeld en de deadlines voor deze taken vastgesteld. Een erg handige methode op deze afspraken en deadlines duidelijk te maken is het iemand aanwijzen als notulist. Hij of zij zal dan alle punten die besproken zijn in dit overleg netjes notuleren en dit naar elke bank opsturen, zodat er ook geen onduidelijkheden kunnen voorkomen. Het volgende overleg start met een korte evaluatie van de afgelopen dagen. In deze evaluatie wordt de verschillende kennis die elke bank heeft opgedaan gedeeld in dit overleg, zodat elk groepje deze kennis nuttig kan gebruiken.
Als een groepje ergens niet uitkomt, dienen zij dan dat ook gelijk aan te geven, zodat er zo min mogelijk tijd verloren gaat. Wellicht is er een collega van een andere bank die zij daarmee kunnen helpen.

Literatuurlijst

https://en.wikipedia.org/wiki/Man-in-the-middle_attack
https://www.lookingglasscyber.com/blog/atm-hacking-you-dont-have-to-pay-to-play/
https://securitytrails.com/blog/security-through-obscurity
https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
https://www.byte.nl/kennisbank/onderhoud/gegevens-beveiligen-met-encryptie-en-hashing
https://www.vtmgroep.nl/kennisdossiers/ict-security/wat-is-een-ddos-aanval-en-hoe-kan-ik-ddos-aanvallen-voorkomen