Beveiligingsrapport

Beveiligingsrapport van: Robert-Jan Schutte (1035471) Rowan van der Zanden (1027332) Stefan Böhm (1023752) Yordi Butter (1034877)

- Data Flow Datagram

Zie bijlage.

- Risicoanalyse:

Fysiek:

1. Informatie op de pinpassen kopiëren met een RFID-scanner.
2. Pincode stelen door niet goed afgeschermde pinautomaat (shoulder surfing).
3. De ATM kan door iedereen open gemaakt worden.
4. De ATM kan makkelijk verplaats worden door iedereen.

Digitaal:

5. Packets intercepten en de gevoelige data van de gebruikers stelen.
6. SQL-injection met de een RFID pas.
7. Een oud medewerken heeft nog steeds toegang tot data.
8. Een toegangwachtwoord wordt geraden.

- Maatregelen:

1. Zo min mogelijk data op de pas zelf zetten.
2. De klant de pincode laten veranderen wanneer zij het gevoel hebben dat dit is gebeurd en de keypad goed afschermen door niet alleen de ATM zelf maar ook de gebruiker die dit zelf kan afschermen.
3. Een deur aan de achterkant maken die alleen toegang geeft wanneer iemand bevoegd is.
4. De ATM in de muur monteren/van staal maken (dit is niet binnen de scope van deze opdracht).
5. Gebruik maken van HTTPS zodat de data niet te lezen is.
6. Zorgen dat de bankserver de inputs sanitized en zo SQL-injections eruit haalt.
7. Wanneer een medewerker een andere functie krijgt of niet meer bij de bank werkt, de bevoegdheden aanpassen of verwijderen.
8. De eisen zetten dat een wachtwoord zowel letters nummers als tekens bevat en deze regelmatig laten veranderen.

Advies

Onderzoeksvragen:

- Is er nagedacht over SQL injection?
- Is de data die naar en van de bank komt beveiligd?
- Wordt er niet onnodige data verstuurd?
- Is er een manier om malware op de ATM te zetten(bijv een usb poort)?
- Is de ATM zo gebouwd dat inbraak moeilijk is?

Ons advies aan groep 3: Money Bank (MNBK) is:

- Zeer uitgebreid en ziet er inhoudelijk goed uit.
- Bij de dataflowdiagram word de hardware gegroepeerd onder Graphical User Interface (GUI) i.p.v. User Interface (U.I.) of een andere generieke term voor de hardware.
- De dataflowdiagram mist de NOOB server binnen het systeem
- Er worden mogelijke oplossingen gegeven die voor ons niet realistische op te lossen zouden zijn.
- Voor de leesbaarheid, zet het wat minder op elkaar. Geef ruimte aan je alinia's

Ons advies voor de landsbank is:

Zorg voor een veilig verkeer van data

Blijf in gesprek met de losse banken om een landsbank te maken die goed aansluit.

Zorg dat de landserver op de noobserver aan kan sluiten zonder extra verwachtingen van andere partijen.

Onze bank gaat bijdragen aan de landserver door te helpen met de ontwikkeling van de database en door aan code te werken.

Bibliografie

Galluccio E, Caselli E, Lombari G, Safari, an O'Reilly Media Company. Sql Injection Strategies. 1st ed. Packt Publishing; 2020. https://go.oreilly.com/queensland-university-of-technology/library/view/-/9781839215643/?ar. Accessed April 22, 2022.

Thornton F, Haines B, Das AM, Bhargava H, Campbell A, Kleinschmidt J. Rfid Security. Rockland, MA: Syngress Pub; 2006. INSERT-MISSING-URL. Accessed April 22, 2022.

What is Shoulder Surfing ? | Shoulder Surfing Explained | Security Wiki (doubleoctopus.com)

Date	Version	Description	Author
4/22	1.1	Finished document writing document and citing sources	Robert-Jan
4/21	1.0	Created document, started doing research and writing the document	Robert-Jan