Case Study 2 – Security Management

Media storage service



Project Members & Student Numbers:

* Kaloyan Andreev (4408020)
* Francisco Marcó (4467752)
* Sava Vasilev (4663438)

Elaboration Date: 12/06/2022

Group 10

Table of content

[1. Treat actors and their motivation 2](#_Toc105944116)

[2. Security requirements (CIA triangle) 2](#_Toc105944117)

[3. Risk and possible impact 2](#_Toc105944118)

[4. Mitigation 3](#_Toc105944119)

# Treat actors and their motivation

* 1. **former developers and competitors (high risk)**
     1. to hurt the revenue and status of the app application - (former developers)
     2. reduce the competition and hurt the revenue and status of the application - (competitors)
  2. **foreign nations and criminal hackers (low risk)**
     1. provide security and deterrent in case of an altercation between nations – (foreign nations)
     2. earn extra money – (criminal hackers)
  3. **criminals and hacktivists (medium risk)**
     1. earn money – (criminal)
     2. fight for a cause – (hacktivists)

# Security requirements (CIA triangle)

|  |  |  |  |
| --- | --- | --- | --- |
| Company data | Data elements | Data classification  (C.I.A) | Explanation |
| Clients’ information | Name  Email  Phone number  Username  Password | H, H, M | Classification and integrity are important because the clients’ data can be leaked. They present a security risk as well. |
| Log records | Dev. IP  Account ID  Time  Data | M, M, L | Important for technical or forensic research. Less important for business continuation. |
| Files’ information | ID  Username  File name  Type  Directory | H, M, H | Availability is highly important otherwise the users will not be able to management their data. |
| Backups | System state (files) | H, H, H | Need to be constantly available for disaster recovery and access to them must be limited. |

# Risk and possible impact

1. **Data loss / corrupt data (treats)**
2. Low (probability %)
3. High (impact)
4. Acceptable risk – 2
5. Explanation – Although unlikely to happen, it will still be devastating for the company.
6. **Data leaked**
7. Medium (probability %)
8. High (impact)
9. Unacceptable risk – 3
10. Explanation – Much more likely to happen than data loss and could cause severe financial damages to the company.
11. **Unauthorized access**
12. High (probability %)
13. High (impact)
14. Unacceptable risk – 5
15. Explanation – Out of all the threats, this is the most likely to happen and with highest possible impact. Therefore, we cannot compromise with that.
16. **Power loss / hardware failure**
17. Low (probability %)
18. Medium (impact)
19. Acceptable risk – 1
20. Explanation – Chances are statistically low. To prevent that there is backup power supply. If it does happen though, damages will not be severe.

# Mitigation

|  |  |  |  |
| --- | --- | --- | --- |
| Deterrent control | Preventive control | Detective control | Corrective control |
| Corrupt / loss data | Create a backup policy | Integrity check | N/A |
| Brute force attacks | Complex and hashed passwords | Implement Brute force attacks detection system | Limit login attempts |
| DDoS attacks | Close irrelevant ports | Implement DDoS attack detection system | Purchase DDoS mitigation equipment |
| SQL injections | Good programming | Implement SQL attack detection system | Improve script |
| Phishing attacks | CA Certificates | Phishing attacks is registered as an intendent | Update CA Certificates |