Security management analysis

In this document, the outcomes of our security management analysis are displayed and grouped together.

Threat actors and their motivation

Threat actors are people who execute cyberattacks, take ‘revenge’ on companies of hack sites and applications for their own goods. These actors want their victims to pay them big amounts of money in order to remove the virus or stop the hacks. In some cases, the attacks are purely because of spite because of firing an employee, for example. In this case, it is pretty difficult to predict the threat actors and their intentions because our client, Make IT Work4U, is going to use our server for their own clients. A threat actor for a bank can be someone who just wants to get money from them. An actor for a law firm on the other hand, might wants to change documents to get someone out of jail earlier. As mentioned above, it is pretty hard for us to predict the possible threats since we don't know which companies are going to use our server infrastructure.

The direct thread actors for us, could be people who would like to get ransom money by shutting down our, and our clients’ systems. They could also try to find the weak spots in our system in order to invade on of our clients directly.

security requirements

C- Confidentiality = how private the data is

I- Integrity = importance of data correctness and accuracy

A- Availability = importance of system availability

|  |  |  |  |
| --- | --- | --- | --- |
| Company data | Data elements | Data classification  (C, I, A) | Explanation |
| Account information | Login ID and password | H, H, H | Account availability is critical for employees and admins. Account confidentiality is critical because accounts provide access to various sorts of confidential information. |
| Log record | Date  Type  Time  event | M, M, L | Auditing and technical or forensic research require log recordings. Less critical for business sustainability. |
| Customer information | Email  Name  Id  address | M, H, M | Integrity is essential since errors might result in delivery errors that can jeopardize the company's reputation. |
| Remote connection | VPN login credentials | L, L, L | It is not critical to be able to login remotely; even if VPN config files are obtained, hackers will still need access to the Windows Virtual Machines to steal information. |

L-low; M-medium; H-high;

Risks and possible impact

Here you can find the predicted risks and their possible impacts on our systems and our direct and indirect clients.

|  |  |  |  |
| --- | --- | --- | --- |
| Threat | Probability | Impact | Needed security level  (Probability \* impact) |
| Fraud | Medium/high1 | unknown1 | Depends on company |
| Script Kiddies | High | unknown2 | Depends on company and script |
| Espionage | Unknown but plausible | Medium3 | Low (background checks, watermarks) |
| Abuse of customer accounts | Unknown1 | Unknown1 | Depends on company |
| Account theft/ID fraud or credit card fraud | High | Company/client = high  Customer = (very) high | High (top level and up-to-date) |
| Complete server take-over | Low | (very) high | High (top level and up-to-date) |

1 = Depends on the client and their customers' information  
2 = Depends on the used script and the threat actors' demands  
3 = Depends on the companies' products and the effect