Security management analysis

The outcomes of our security management analysis are presented and categorized in this paper.

Threat actors and their motivation

Threat actors are individuals who conduct cyberattacks, seek 'vengeance' on businesses or hack websites and services for their own gain. These perpetrators demand large sums of money from their victims for a ransomware decryption key, for example. In certain instances, the attacks are motivated only by revenge, such as the firing of an employee. In our scenario, predicting threat actors and their objectives is quite challenging as our client, Make IT Work4U, will be using our server for their own clientele. A threat actor for a bank could be only interested in obtaining money from them. On the other hand, an actor for a law firm may wish to alter documents to get someone out of jail sooner. As indicated previously, it's difficult for us to foresee potential risks because we don't know which organizations will use our server infrastructure.

For us, the direct threat actors may be those seeking ransom money by shutting down our clients' systems. They could even attempt to identify weak points in our system to directly infiltrate one of our clients.

security requirements

A list of (data-)assets is not possible at this time because we do not know who the clients of Make IT Work4U will be.

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 credentials | M, 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

Mitigations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Fraud | Repressive | Preventive | Detective | Corrective |
| Technical |  | Biometric Authentication |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Script kiddies | Repressive | Preventive | Detective | Corrective |
| Technical |  | Antivirus | Checking logs | Restoring backups |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Espionage | Repressive | Preventive | Detective | Corrective |
| Technical |  | Background checks and watermarks in digital environment | Keep checking for leaked intel | Encrypt as much as possible and fire employee if necessary |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Abuse of customer account | Repressive | Preventive | Detective | Corrective |
| Technical |  | Regular password changes | Keep an eye out for suspicious purchases or (trans)actions | Cancel the order, block out the account and notify the customer |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Account theft/ID fraud or credit card fraud | Repressive | Preventive | Detective | Corrective |
| Technical |  | Encrypted storage of sensitive data | Checking activity of account | Password changes on a regular basis |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Complete server take-over | Repressive | Preventive | Detective | Corrective |
| Technical |  | 2 Factor Authentication, regular password changes | Keep monitoring the servers and KPI's on the dashboard | Restoring backups |