**Security risk assessment**

A\_ Discuss the most critical assets of the Warmaksan's system, considering their CIA principles in mind.

|  |  |
| --- | --- |
| **Asset Name (including the CIA)** | **Justification for why it’s critical** |
| The confidentiality and integrity of the existing devices(endpoints) | The data that would be traded from/in to those devices it’s sensitive data that must be protected |
| The availability and reliability of the existing devices (endpoints) | The process of those devices mustn’t be stopped without any obstructions. |
| The confidentiality and integrity of the Monitoring station’s data | The attack on a single subnet could lead to impact on the Secrecy of the data and the possibility of make any change on it |
| The availability and reliability of the monitoring devices | These security networking devices should be separate of any other subnets to avoid goes them down and to not rely on them. |
| Confidentiality, integrity and authenticity of The Data for each branch | It’s the most sensitive assist because it has high values also sensitivity specially when it’s transferred. |
| Confidentiality and integrity and availability of the web services | With the web protocols the data will transferred so it has to be so secured to transfer the data to the cloud |
| Confidentiality , authenticity and availability of the users data | The data of the users it’s sensitive so it’s must the transmission be fully secured |
| The authenticity and accountability of the door system in the data center | It’s not make any sense to permits anybody to access to data center it’s the most physical security layer restricted, that should contain several authenticity steps. |
| Accountability, authorization, integrity and confidently of the accessing the data center via VPN | Not anybody has the authorized to access the data center even by some services such VPN and to be sure the application that would run which fully secured |
| Authenticity and accountability of the third parties for supporting VPN | to be the third parties trustworthy enough to support the VPN |
| Confidentiality, integrity and Authenticity of the misconfiguration data of the firewall and VPN | The misconfiguration could have services permissions furthermore inconsistence authentication. The misconfiguration can open the gate for the external hacker to be in your network as that hacker connected physically to your network |
| Confidentiality and integrity of the unpatched applications and services | That mean there’s a vulnerability that the enterprise already knows about it and didn’t get fixed. |
| Confidentiality, integrity, authenticity and accountability of the password polices | The password is important authenticity of the accessing so it must have a clear policy must follow from everybody if there’s an issue it could lead to accessing to the system non-authorized. |

B\_ Suggest (given the notes above) the possible controls/countermeasures initially used by the company to protect their asset.

|  |  |
| --- | --- |
| **Asset Name (including the CIA)** | **Controls initially used by the company** |
| The confidentiality and integrity of the existing devices(endpoints), The availability and reliability of the existing devices (endpoints) | No control |
| The confidentiality and integrity of the Monitoring station’s data ,The availability and reliability of the monitoring devices | Monitoring station of the whole system |
| Confidentiality, integrity and authenticity of The Data for each branch , | Database servers |
| Confidentiality and integrity and availability of the web services | Database servers |
| Confidentiality , authenticity and availability of the users data | Database servers |
| The authenticity and accountability of the door system in the data center | Doors |
| Accountability, authorization, integrity and confidently of the accessing the data center via VPN, Authenticity and accountability of the third parties for supporting VPN | No control |
| Confidentiality, integrity and Authenticity of the misconfiguration data of the firewall and VPN | firewalls |
| Confidentiality and integrity of the unpatched applications and services | Servers |
| Confidentiality, integrity, authenticity and accountability of the password polices | Password polices |

C\_ Discuss and assess Warmaksan system's possible risks, their likelihood (**rare, unlikely, possible, likely, and almost certain**), and exploitation consequences (**insignificant, minor, moderate, major, catastrophic, and doomsday**).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset Name (including the CIA)** | **Possible Risks** | **Impact** | **Likelihood** | **Justification for likelihood and impact** |
| The confidentiality and integrity of the existing devices(endpoints) | Attacks and malwares | Insignificant | Likely | If there’s some endpoints the impact of it could be during a week or less and the attack will not be surprised if happened |
| The confidentiality and integrity of the existing devices(endpoints) | Using an outdated malwares or didn’t use it at all | Minor | Likely | The malwares are continuously so there’s no solution but the only one thing to resistance is to have anti-malwares that save you of losing data or much more the impact is on one area and takes less than a week with high probability to happen |
| The confidentiality and integrity of the existing devices(endpoints) | Not using a strong password | Insignificant | Almost certain | The weak password by guessing can easily pass and get the accessing to the devices and all the data |
| The availability and reliability of the existing devices (endpoints) | Natural disasters | doomsday | Rare | The impact of a natural disaster could be destroyable of the business and huge loss of the equipment but it’s rare specially in the datacenter (Singapore) that consider the 13 of lowest possibility of happened a natural disaster around the world and for that reason it’s rare to happen |
| The confidentiality and integrity of the existing devices(endpoints) | Transform the devices to zombies and bots  (related to the availability and authenticity of the datacenter) | Moderate | Possible | the impact can make the servers down and that could happen with the contribution of the zombies and bots(the devices ). |
| The availability and reliability of the existing devices (endpoints) | fire that could burn the devices | Catastrophic | Possible | The fire have the higher possibility to happened than natural disaster but the impact could be less than the natural disaster |
| The confidentiality and integrity of the Monitoring station’s data | LAN attacks that effect the monitoring station(man in the middle ) | Major | Possible | If the attack happened in the LAN so the data of the monitoring station of the system will be for sure in a serious danger and the possibility is still stand if you don’t have the right distribution of the LAN |
| The availability and reliability of the monitoring devices | Electric interruption and make them down | Minor | unlikely | The electronic interruption could happen because of external consequences but the impact of it not |
| Confidentiality, integrity and authenticity of The Data for each branch | DOS and DDOS attacks | Major | Likely | A website like Donzal it will absolutely have attack such a DOS and DDOS attacks that has a sensitive data like account of Politicians that enough to be targeted specially the datacenter but it could effect on the servers to make them down |
| Confidentiality and integrity and availability of the web services | Web spoofing | Doomsday | Unlikely | The type of data that would be send on the web application and protocols it’s extremely sensitive so it must be well secured to less the possibility for the lowest level. |
| Confidentiality , authenticity and availability of the users data | Web spoofing | Catastrophic | Unlikely | The data of the user is too value and sensitive and it’s include of the data of the of each branch it must be secured . |
| The authenticity and accountability of the door system in the data center | Access by spy or a hacker | Major | Almost certain | There’s no door system so can anyone access to the data center the likelihood is almost certain the impact is big because the unauthorized person is in the most sensitive place in the whole enterprise. |
| Accountability, authorization, integrity and confidently of the accessing the data center via VPN | Run a malwares in the data center | Catastrophic | Possible | The possible is consider high level and it depends the VPN is it from a trustworthy provider and the consequence could destroyable specially the malware run on the brain of the enterprise (data center). |
| Accountability, authorization, integrity and confidently of the accessing the data center | A terrorism armed attack | Catastrophic | Likely | Donzal has so sensitive data as we mention such Politicians and public figure so don’t be surprise to receive any armed attack to seizes the |
| Authenticity and accountability of the third parties for supporting VPN | able malwares to be in the system | Major | Possible | The third party could able the malwares to your system and stop an important service that the company has which is VPN and that is high possibility. |
| Confidentiality, integrity and Authenticity of the misconfiguration data of the firewall and VPN | Allow the packets could contain some malwares | Moderate | Possible | The damage is intermediate but the likelihood is high |
| Confidentiality, integrity and Authenticity of the misconfiguration data of the firewall and VPN | Send packets to wrong directions |  |  |  |
| Confidentiality and integrity of the unpatched applications and services | Exploiting a vulnerability by an attacker in a services or an application | Major | Possible | The impact of it is to accessing and control the applications and services but if didn’t patch it so the level of risk will still high |
| Confidentiality, integrity, authenticity and accountability of the password polices | Week password polices | Minor | Unlikely | The password is taken care of it by most of enterprises so the likelihood is low and the impact could be intermediate. |

**Final Risk Registry**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Asset Name (including the CIA)** | **Possible Risks** | **Existing Controls** | **Impact** | **Likelihood** | **Risk Level** | **Priority** |
|  |  |  |  |  |  |  |