Risk Management Priorities

Student’s Name

Institution Affiliation

Risk Management Priorities

In my organizations, some of the main assets include computer devices, stationaries, network devices, and appliances. Most of the activities undertaken in my organization are conducted over the internet. The organization also has a network, where different computer users can access data from a centralized location. Some of the assets and their vulnerabilities are listed below:

|  |  |  |
| --- | --- | --- |
| **Asset Listing** | **Vulnerabilities** | **Risk-rating value** |
| Desktops | Virus attacks from the internet. Threat from the use of other devices such as flash disks from outside. Risk of computer hacking. | 9.0 |
| Laptops | Threats from outside devices such as flash disks. Virus and malware from the internet. Due to its portability, they face the risk of outsiders accessing company data. | 9.5 |
| Servers | Unprotected local data, server hacking, infected files going to the server, unauthorized access. | 9..5 |
| Routers | Default passwords, password leakage, password sharing, weak firewalls. | 7.5 |
| Printers | Wireless printers can be hacked, thus giving access to other computers. Printers don’t have antimalware services. | 7.5 |
| Network storage | Hacking from cybercriminals | 8.5 |
| Cameras | Remote access encouraging spying activities | 7.0 |

**Summary and rationale of the ranking**

Since most of the work conducted in our organization uses computers, I find that the organization faces a huge threat from cyber vulnerabilities. Moreover, the computers are connected via a network to allow for easy transfer of files from alone user to the other. For this reason, if one computer gets infected or attacked, the whole organization is put at risk. Such a threat makes computers in the organization very risky, and thus the high rating. For laptops, they are riskier than desktop computers, since they are mobile. Some of the workers have been permitted to carry their laptops when meeting with clients outside the organization. The portability factor of the laptop means that it will be exposed to other networks, Wi-Fi signals, thus making it more vulnerable.

The server and network storage play a significant role in our organization. It is where most of the company data is stored. If the server was attacked or hacked, it may result in significant losses to the company. Other workers in the organization are connected to the server with different levels of permission. All relevant data are stored in the server, therefore any damage to the server may halt the organization’s operations, thus making it to have a high score.

For routers, they play a crucial role in ensuring the internet is well distributed in the entire organization. With the provision of Wi-Fi services, routers play a crucial role in connecting wireless devices to the network. If the authentication procedures are not secure enough, hackers may take advantage and exploit the router’s vulnerability, to access the organization’s data. Ensuring that authentication procedures such as passwords are strong will ensure the organization’s safety.

Printers have recently become a target for hackers because in most cases, printers do not have protective features like installing malware software. Moreover, smart printers are now wireless and smart, which means that they can be connected to every single simultaneously. Such features make it a target for hackers, where they use various exploits to access the printer, thereby accessing the connected computers. For this reason, printers present a considerable level of threat, and thus the score of 7.5.

Cameras have also become a target for hackers. Cybercriminals may use their ingenuity to remotely access the organization’s camera to spy on the workers or the management. The act of spying can reveal crucial information such as routines, details on where files and other items are stored, location of a safe, and other crucial information that may aid criminals (Arsene, 2019).

References

Arsene, L. (2019). Vulnerabilities in smart IP cameras expose users to privacy, security risks. *IT* Portal. Accessed May 15, 2020, from <https://www.itproportal.com/features/vulnerabilities-in-smart-ip-cameras-expose-users-to-privacy-security-risks/>.