Security Report

Student’s Name

May 22, 2019

**Securing computers for the Marketing department**

There are numerous ways that the marketing department can do in order to provide the required security for the computers which support the department operations. The following are some of the major recommendations(Geier, 2014);

Define and implement **system access levels** to both the computers and the organizationnetwork. This would act as the first barrier to preventing any unauthorized access to the department organization computers. Use of access level helps secure the computers in the marketing department by limiting access to various resources of the marketing department and also the organization network. In this case, the user would be ableonly to access what they are authorized to get.

Make sure that all the computers within the organization and most specifically, the marketing department have been **installed with current and up-to-date antivirus and all their software are updated**. In this case, any device connecting to the organization must have up-to-date antivirus, this is important as it would help scan and prevent any malicious activity within the organization network and thus help secure the organization computers. Use of updated software help patch any security vulnerabilities which are already known and thus helping secure the marketing department computers.

Other recommendation on how the marketing department can secure their computers in relation to the organization network and servers includes, implementation of password policies, educating the employees on the social engineering, use of backup and recovery for both the organization and individual employees, use of VPN and ensuring that the network and the network software such as the firewalls are up-to-date, (Geier, 2014).

**Securing Network Traffic Within the ABC, Inc.**

The following security recommendation can be used to secure the network traffic between the workstations within the organizations;

Performing network audits and mapping within the workstations within the building and the server, this is necessary as it might help reveal some hidden vulnerabilities within the network and which might pose as security threats to the organization network.

Keeping the network hardware and software up-to-date, this includes all the firmware such as firewall and others. Keeping all the network infrastructure and resources updates ensure that there no known vulnerability that can disrupt the network flow within the organization and thus ensuring that everything is secure(Geier, 2014).

Other ways of securing the network flow between the workstations within the building and the server include physically securing the network infrastructure, mac filtering to ensure that only organization employees can access the network and eventually considering the use of VPNs

**Trust boundaries**

Trust boundaries such as the end system devices such as the employee’s computers and other network devices can be filtered using Mac address to ensure that only the required devices are allowed within the network. Also, the trust boundaries levels can be implemented using the access switch and distribution switches in order to ensure the highest level and lowest level access, such as phones have the required access bandwidth. The distinction between the highest level and lowest level in trust boundary includes the priority based on the activity within the organization.

**Measures to harden the server OS**

There are various ways that the ABC, Inc. organization administrator can do in order to increase the security of the organization information resources through the hardening of the OS. This includes Removing any unnecessary programs within the Server OS and which has no role within the organization. Disabling any unused ports, services, and accounts within the Server OS, set up the access controls and use the service among other security measures.

The Server administrator should make use of services such as the readily available service parks which are provided by the OS providers. Other security services which can play a role at the hardening of the OS includes the use of security templates which can be used to configure the policies and configurations automatically.

On both the Server and the organization workstations OS, patch management policy can be of much help as it would help prevent any future targeted malicious activities among other security issues. Policy such as patch management can be used in this case there should be the appropriate patch and update planning, testing, implementing and eventually the auditing of the patch to ensure that it acts as it is supposed to act, also there should be a policy which outlines when and how the OS patches would be applied, (Smith, 2016).

**Securing the organization database**

The organization database can be secured by the use of encryption where necessary, (Rubens, 2016),the grant of roles and permission to the authorized database users as outlined in the chart below.



**Implementation Process and Timeline**

|  |  |  |
| --- | --- | --- |
| Activity | Implementation process | Timeline |
| Securing the marketing department computers  | Access levels, installation of antivirus software, Configuration of firewalls, password policies, backup and restore, among others.  | Two weeks |
| Securing Network Traffic.  | Defining trust boundaries.Network audits and mappings.Physically securing the network and updating the network software | Two weeks |
| Hardening the server OS | Removing unnecessary programs and cleanups.Applying of OS patches and updates | One week |
| Securing the Organization Database. | Adding the user groups.Adding the departments and the database sharing groupsGranting the required roles and permission.  | One week |
| Testing  | Testing the new security implementations  | Three days  |

**References**

Geier, E. (2014, 3 17). Retrieved from https://www.networkworld.com/article/2175048/8-ways-to-improve-wired-network-security.html

Rubens, P. (2016, 8 23). Retrieved from https://www.esecurityplanet.com/network-security/6-database-security-best-practices.html

Smith, H. (2016, 11 9). Retrieved from https://www.continuum.net/blog/6-important-steps-to-harden-your-clients-operating-systems