SYSTEM DOCUMENTATION

RIHAM AHAMED ABDUL RAHEEM
HND COMPUTING IDM

Contents

GENERAL GUIDELINES

- Watch Officers are granted the task of initial recovery troubleshooting for the network. they're going to be treated because the administrators of the network and be granted with a private user account to the server, but they're going to not have permissions to delete any files on the server.
- Civilian staff doesn't have permission to access the server room.
- Civilians must adhere to and obey all procedures declared by watch officers within the case of a network emergency.
- The watch that's under each watch officer will interact with the civilian staff if they require any information a few particular situation, they have not interact with the clients within the network.
- The Chief Fire Officer is that the only administrator that has all permissions to work the server on a medium-scale without altering any network software infrastructure..

HARDWARE DESIGN PLAN

All switches which will be used must be level 3 manageable switches; they need to be connected with RJ45 cables and be connected to a router, then through a firewall to the server.

1. The center are going to be equipped with 3CX IP phones which will allow direct calls from public liaisons, police and the other foreign base that the hearth department is liable for .
2. The watch officer should be equipped with a 3CX softphone in the least times. this is often in order that the watch officer is instructed by the center in the least times.
3. The controllers should have their softphone equipped and have an IP enabled hard phone by them in the least times.
4. All systems within the center must be networked and plugged into a 16 port level 3 switch. Only 3 are going to be used but just in case the center is expanded the switch doesn’t need to get replaced .
5. All switches and routers must be rack mounted and be fitted with patch panels and successively plugged with keystones in order that the ports aren’t damaged.

6. The civilian client systems must be networked through a 16 port level 3 switch, and connected to the router.
7. The civilian client systems must have a networked IP enabled printer to require any printouts.
8. To take care of 2 way communications between within the vehicles, a 3CX IP hardphone must be placed with additional speakers and a softphone stored inside each vehicle.
9. All vehicles must be fitted with GPS units, all monitoring must be done by the three controllers within the center .
10. The center will contain the rack mounts which will have all the network devices but under lock and key, the key should be with the one among the administrators.

HARDWARE DISASTER RECOVERY

1. within the event of a natural disaster, the administrators must take an inventory of all damaged devices and replace them immediately per the service agreement with the hearth department's network device providers.
2. within the event of a security breach, the administrators of the network must immediately take necessary logs of the network that specify the breach, then temporarily disable all access to the server till the breach has been mitigated. In such instances if the administrators cannot get over the breach, the network administrator must be immediately involved .
3. within the event of bad connectivity or cable damages, administrators are forbidden to aim anything. The network administrator must be contacted and tend this technique documentation, per the documentation and these failsafe protocols, he's to research , log then repair the difficulty .
4. within the event of the identification that a networking device isn't functioning properly, Chief Watch Officer must contact a network technician from the provider then ask them to verify the matter , log it then proceed to repair it. If the matter is unfixable then the network administrator should either plan to replace unit itself or the device.

SOFTWARE DESIGN PLAN

1. All client systems must be installed with MalwareBytes Business version, and configured to scan once in every 3 days.
2. The server must be installed with Windows Server 2012, and therefore the administrators are alleged to update it as soon as an update is out there but a system restore point must be created and protected .
3. The network administrator must use WireShark to smell packets getting into and out of the server to see if the networking is functioning because it is meant once in hebdomadally .
4. All client systems must be installed with Windows 8 licensed versions and updated when updates are available.
5. The client systems must be restricted from surfing the web unnecessarily, only department websites, services and related interfaces must be allowed to be searched.
6. If a client system is infected by any sort of virus, then until the danger has been mitigated all notably infected client systems must be disconnected from the network.
7. Administrators must make regular backups of the content within the server, and store them in auxiliary storage devices stored under lock and key.
8. All sensitive soft information must be encrypted with AES 256-bit in CCM mode with randomly generated 8 alphanumeric character passwords.
9. The passwords of the client systems must be changed once in monthly .
10. Server administrator passwords must be changed once in every 2 weeks.
11. Server administrators are only given permissions to read and modify files within the server, with the exception of Chief Watch Officers.
12. All client systems can only access the server to read and download files from the server.
13. All the hearth department staff must be trained properly by the network administrator and his staff, whenever a replacement implementation is introduced to the network.

IMPROVEMENTS

- The center must be assigned as a separate VLAN.
- The civilian office must be assigned as a separate VLAN.
- A router must be installed to enable inter-VLAN communication between the above stated departments.
- A router with firewall and vpn technology must replace the extra firewall within the server room.
- Distribution of a mobile application which will only call the hearth department within the case of an emergency.
- Control center staff must be increased so as to make sure maximum efficiency during work.
- All client users must be denied of plugging in any external media to the client systems.
- A hybrid topology of bus and star must be implemented, bus within the civilian office and star within the center then directly connected to the router within the server room.
- A physical security expert must be hired to carefully increase the physical security of the hearth department in such how that the network's maximum security is ensured.
- Mitigation from local storage to cloud storage, which will store all information encrypted and hashed.
- A Metropolitan Area Network is meant in such how that the hearth department can directly communicate with the police and other emergency services.
- A Wireless Access Point must be introduced within the civilian office in order that staff is inspired to use their own devices to access the network rather than client systems.
- IPSec must be implemented when the newtown local department communicates with external services just like the police in order that sensitive information isn't sniffed.