Willis Consulting of York

Willis
Consulting of York

System / Network Assistment

Company:	York Business and Industry

Date: 4/28/2010

Address: 123 Business Centre
York, PA 17405

Phone: 717-745-1234

Network (Mixed):

Microsoft Windows Server 2008 Active Directory and Remote Desktop Services
Red Hat Linux Servers
3COM 10/100 Switched Ethernet, CAT5
100FX Fiber Ethernet connection 3 Wiring Closets
AT&T T1 Internet Service

Servers and Services:

1. **Dell PowerEdge SC440**, 8GB RAM, Windows Server 2008 R2, BDC

   Windows IIS – Hosting company's Internet Site www.yourkbusiness.com

   MS Exchange 2010 – Hosting Company's Email @yorkbusiness.com

   Approximately 75 User Accounts

2. **Dell PowerEdge 7900**, Windows Server 2008 R2, PDC

   - Windows File and Print (approximately 25 attached printers)
   - MS SQL Server Express – Servicing Time Clock Application
   - Solid Works Licensing
   - remote Desktop (Terminal Services) Licensing
   - Epicor ERP Software

3. **Micron Millennia Workstation**, Red Hat Linux

   File Server for CAD drawings

4. **Dell PC**, Red Hat Linux

   Firewall

5. **NAS** Ethernet Attached, 2TB Drive

   Back-up of Epicor and CAD drawings

Willis Consulting of York

System / Network Assistment

Topology Summary:

Most users connect to the PDC using Terminal Services and Thin Clients.

Email is connected via Outlook to the Exchange Server using cached OST files.

Remote Users can connect to the Remote gateway and connect to their RDC.

Antivirus is through Symantec Endpoint which provides Antivirus, Antispyware, Firewall, Intrusion Protection, and Malware control.

Backup is performed daily to the Ethernet attached 3TB NAS

The PDC and BDC have RAID redundancy.

Epicor provides the companies ERP control and is the primary used software, using a SQL database that can be backed up live.

Systems Evaluation:

1.   The Dell Power Edge 7900 is essentially the computer on network. It is over utilized with a complexity of applications and is experiencing frequent problems requiring rebooting during normal operating hours.

   It functions as the primary domain controller, which handles all users logins, managed rights, system policies, system and software updates. It also provides all DHCP IP addressing.

   It functions as the Terminal Server which runs an instance of window for each user and runs the instance of any application such as MS Word. When connected to Terminal Services the only function that the client PC is for mouse and keyboard passes the screen image. It also manages the Terminal Services Licensing to control who and when can connect.

   It functions as the SQL server database and hosts the Time Clock application.

   It handles all 25 printer queues.

   It is running Symantec Endpoint providing all networked Antivirus functions and updates to clients.

   It controls the licensing for SolidWorks.

   It runs your ERP software, Epicor.

2.   Antivirus Security using Symantec Endpoint.

   Symantec Endpoint is a very good Antivirus software. It will monitor both Windows and Linux systems and it also provides intrusion prevention. However, it is not installed on the Linux firewall which is configured as your first line of defense.

Willis Consulting of York

Willis Consulting of York, LLC
1885 Jug Road
Dover, Pennsylvania 17315
Phone: 717-858-9068
Fax: 866-423-7555

System / Network Assistment

Symantec Endpoint also does not have a messaging client for Microsoft Exchange, it will only detect email virus after they have been stored in Exchange and opened to the Client.

3. Internet Content Filtering

    There is no Internet or Email content filtering and monitoring.

4. Remote Connections Virus Checks

    There is no software check for Remote Connections. Not having this allows for a home computer which is infected with a virus, to connect to the network.

5. Backup

    The present mythology is backing up data files and Epicor database files to a connected NAS drive. While making a backup to a NAS device is convenient it is not complete. The NAS drive is itself a hard drive and is subject to failure and has no redundancy. If it would crash, all of your backup would be lost.

    The entire email system is not being backed up at all and could not be recovered it the server crashed.

    There is no offsite storage of any data.

6. Internet Site / Exchange Security

    The Internet site is the most vulnerable security risk since you allow the general public (the entire world) access to this computer. Once compromised, someone would have full access to the network since this is located on a SDC. In addition, access to the Exchange email is on the same computer.

7. Network Diagram

    There is no complete wiring diagram. A diagram drawing of the Network including the IP schemes, wiring closets and terminal numbers will improve network maintenance and avoid many problems.

Proposed Changes:

1. Install Microsoft Forefront Server.

    Benefits: The Forefront server serves as a frontline defense from the internet. It has built-in functionality to handle Internet requests for your website and Remote Desktop Connections instead of these being passed inside your network. It supports several network cards that can keep your website separate from your network. You can also install Websense to monitor and filter Internet connections. Symantec Enterprise also gives you a frontline defense before anything reaches the inside of your network.

System / Network Assistment

2. Install an Enterprise Backup USB Drive system

    Benefits: This will provide a complete GFS backup scheme while providing for a media to be taken off site. It would be used in conjunction with any NAS backup. It will also provide for a backup of Exchange and Outlook email and Microsoft Active Directory so that it could be completely restored.

3. Terminal Serves and ERP Software on Separate Servers

    Benefits: Terminal serves creates a huge overhead of disk and memory on the server and should be hosted alone on a Windows 2003 server. All instances of windows and programs are running on the server and continue to run even when the user logs out.

    Your ERP software is at the core of your company's business. All ERP software should always be hosted alone on a server. Currently your server is being over utilized and this can cause not only performance issues but errors caused by conflicting threads.

4. Application Server

    Typically, companies run all unique applications on a separate server. The reason for this is they require constant updates and require the server to be rebooted more than other servers. If they are on their own server, this can be done with a minimum impact on the network and users.

5. Gigabit Network Switch

    Servers are constantly communicating with each other. Two of your servers are gigabit ready (1,000 bps) and are only connected using a 100 bps switch. This connection could also be used to connect the Designers to the CAD files which can also utilize a lot of bandwidth.

Summary:

The purpose of this evaluation is to root out current or potential issues and suggest necessary changes to address them. The network has many positive points and is generally in good shape. The suggestions will improve the network but may not be immediately implemented but serve as a heading or goal. The three items that need immediate attention is (1) Backup, (2) Terminal services running on an over utilized server and (3) General topology of the firewall.

There are several paths that can be taken and this can be discussed to lay-out a plan that best suit York Business and Industry's goals and budget.

Attached is a simple sketch of how the Network topology should be configured to provide optimum security and reliability.

Prepared by,

Will Parshall
Principal Consultant
Willis Consulting of York, LLC