Global Information Assurance Certification Paper

Kevin Murphy
March 15, 2004
GSEC Practical Assignment, v1.4b - option 2
CASE STUDY: Secure Email Deployment With Windows 2003 and Exchange 2003

INTRODUCTION

A small company that considers email "mission critical" has a very flawed and insecure email infrastructure. Leveraging their previous investments in Microsoft technology, an upgrade to Windows 2003 Server and Exchange 2003 Server can secure their network and encrypt remote email access.

Using Windows 2003 and Exchange 2003 Server I will discuss how to configure and setup a DMZ and host a secure email system on a small corporate network. This system will accept incoming SMTP mail for the company's Internet domain, provide users with SSL encrypted remote access to email via Outlook 2003, and provide a SSL encrypted web-based email access as well.

CURRENT ENVIRONMENT

Murphy Beverage Inc.[1] is a small, national beer distributor with 50 employees and 4 sales offices in Atlanta, Los Angeles, New York and Pittsburgh. Each office has 5-15 employees – mostly salespeople with laptops, plus some administrative assistants with desktops. All workstations are running Windows XP Professional. Email is considered "mission critical" as it is the primary method of contact between employees and with clients.

The Atlanta office serves as the hub of the company's computer network. There are 3 servers in the Atlanta office: a Domain Controller/File and Print Server, a Firewall, and an Email server. There is a T1 Internet connection plus (2) T1 VPN WAN Connections.

The other offices have a T1 VPN WAN connection to Atlanta and 1 Domain Controller/File and Print Server on the local LAN.

All servers are running Windows 2000 Server SP4. Microsoft Exchange 2000 SP3 is the company's email platform (running in Native Mode). Users use Microsoft Outlook XP to access email. Outlook Web Access (OWA) is also enabled for email access via any web browser.

Salespeople are often out of the office. Fast, reliable, secure access to email is expected to be available to all employees in or out of the office. Users connect remotely via company provided dial-up or often via their home cable/DSL ISP's. Increasingly, users are purchasing Wi-Fi cards on their own and using them at public hotspots in airports, stores, parks, and hotels.

This network was originally setup in March 2001. Because of the many features the Outlook client supported that were not available in OWA, management requested a solution that provided Outlook access via the Internet. Per Microsoft KB Article 270836 [2] ports 135, 4000, 4001, and 8801 were configured on the Exchange server and opened on the Firewall (via static Network Address Translation) to allow users to connect with

Outlook to the Exchange server via any Internet connection. At the time the benefit and desire for Outlook access outweighed the risk and threat from opening up those ports. That all changed in August 2003 when the Blaster Worm was released. The company's Exchange server was current on patches and avoided infection. But this method of using Outlook to remotely connect to Exchange quickly became unreliable for many users as their ISP's began blocking port 135 to stop the spread of the worm as recommended by Symantec [3].

OWA was also setup and installed on the Exchange server. This was provided as a secondary method to access email in situations where remote users did not have their company laptop (i.e. conferences, home PC's, or wherever port 135 was blocked). Port 80 was opened on the Firewall to allow these connections through to the Exchange server. Additionally, the OWA website was not using SSL encryption causing usernames, passwords, and messages to be sent in clear text.

The company had considered implementing a front-end/back-end configuration for OWA originally, but Microsoft licensing costs were prohibitive. For Exchange 2000, an Enterprise License was required to configure a server as a Front End server. With Exchange 2003, a Standard license can be used as a Front End server – saving approximately $4000.

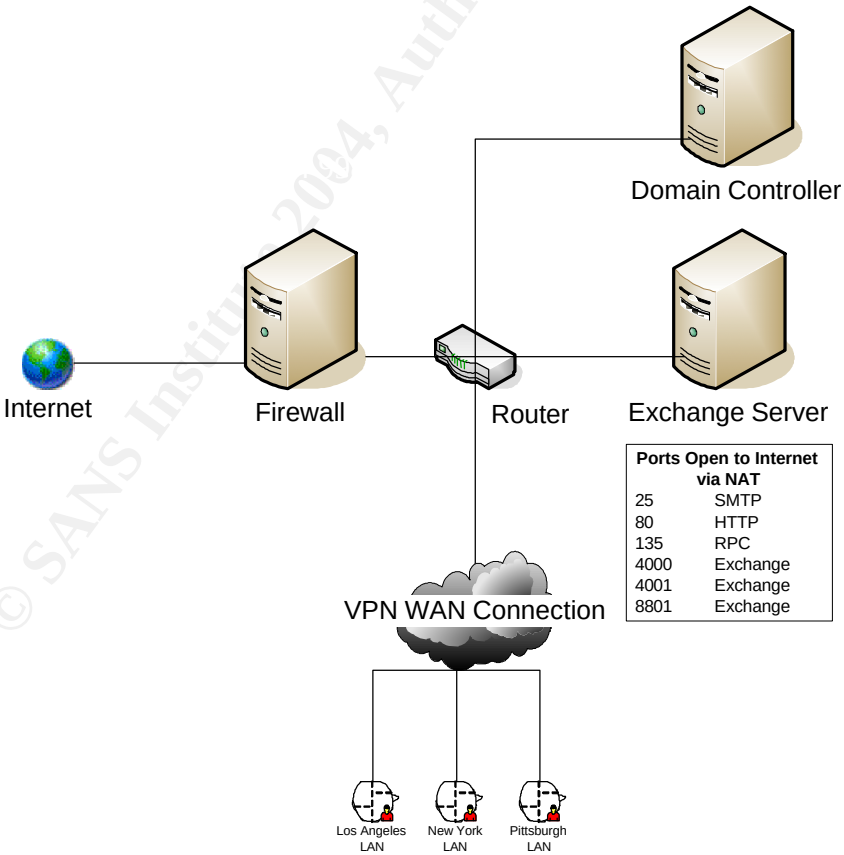

Diagram 1: Murphy's Beverage Inc. "before" network diagram

PROPOSED ENVIRONMENT

Based on the topics from the SANS Security Essentials class, I see 6 fundamental Internet security principles wrong with the "before" design:

1. There is no DMZ for public services
2. Public Traffic is allowed into the internal LAN
3. The company's Exchange server is accepting SMTP mail from the public internet
4. The company's Exchange server is running a publicly available web server
5. HTTP is transmitting usernames, passwords, and other sensitive information over the Internet unencrypted
6. The company's Exchange server port 135 (RPC) is open and exposed to the public internet

The risk of the Exchange server being compromised is very high because of the large number of public services running on it. One of the most often mentioned recommendations at SANS training was to have as few services as possible running on a server and segregate server roles to lessen the number of possible attack vectors. As this is the only Exchange server in the organization, and email is considered so critical to the company, the impact of this server being compromised or losing data is tremendous. The company would be practically shut down until the server could be restored. A disaster recovery plan and daily/weekly/monthly backups, recommended by SANS, do exist.

The first recommendation for the company is to setup a DMZ for their public services. [4] This can be accomplished by installing another network card into the Firewall and configuring a new network. The company already uses the 10.x.x.x subnet internally for servers and workstations. So the 192.168.x.x subnet will be used for the DMZ. The Firewall's NAT rules will be modified to route traffic to the company's public IP address to the new server in the DMZ instead of the Exchange server. This will address the first 2 fundamental issues on the above list.

Next the company needs to evaluate and reconsider their single server Exchange environment. If they add an additional Exchange server, they can utilize the front-end/back-end feature and separate the server roles. One Exchange server would be in the DMZ and one Exchange server inside the corporate LAN. The front-end acts as the SMTP gateway and provides OWA access, while the back-end is behind the Firewall and has the company's actual message store. It is additionally recommended the company purchase a commercial SSL Certificate and encrypt OWA communications with HTTPS. This addresses the 3rd, 4th and 5th fundamental issues on the above list.

If the company upgrades to Windows 2003 and Exchange 2003 Sever they can implement a new feature called RPC over HTTP(S). This allows the Outlook RPC calls (previously using port 135) to be communicated over port 80 like regular HTTP traffic allowing it to pass through Firewalls. This feature can even be used with HTTPS to encrypt and secure this traffic for maximum security. Users will be able to use Outlook 2003 on their laptops and remotely access their email securely from any Internet connection. The old method of remote Outlook access can be closed and address issue number 6 above.

To take advantage of all these new features, Murphy Beverage Inc. will need to upgrade 2 other components of their Infrastructure. The company's Active Directory infrastructure and the Outlook client software need upgrades. The Domain Controller in the Atlanta office will be upgraded to Windows 2003 Server and the workstations will be upgraded to Outlook 2003.

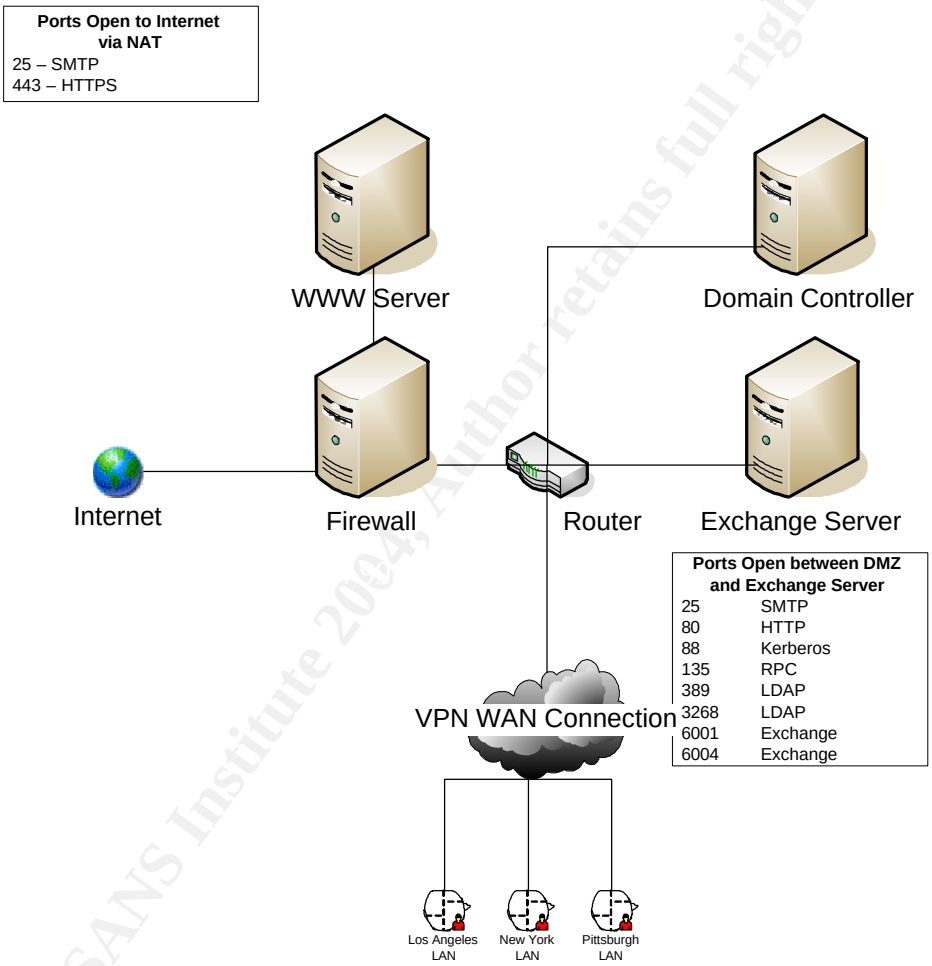

Diagram 2: Murphy's Beverage Inc. "after" network diagram

PROCESS

This section shall detail the individual steps to complete the proposed environment upgrade. These steps will be general in nature and assume that all each previous step completed successfully. Links and additional information will be provided with each critical step to assist readers of this document in preparing for their own upgrade/installation.

Upgrade the Atlanta Domain Controller to Windows 2003 Server:
Two very helpful documents for this process are the Upgrading from Windows 2000 Server to Windows 2003 Server [5] white paper and MSKB Article 555040: Common Mistakes When Upgrading a Windows 2000 Domain To a Windows 2003 Domain [6].

1. Per MSKB Article 325379: How to Upgrade Windows 2000 Domain Controllers to Windows 2003 Server [7] since Exchange 2000 is already installed in the domain, we must modify the Active Directory schema before upgrading to Windows 2003 Server to avoid mangling the LDAP Display Attributes. During the actual upgrade we had issues with this command – this MS Newsgroup Posting [8] helped us get this command to run successfully.
2. Prepare the Windows 2000 Active Directory Forest for the upgrade by running **ADPREP /FORESTPREP** from the \i386 folder on the Windows 2003 Server CD.
3. Prepare the Windows 2000 Active Directory Domain for the upgrade by running **ADPREP /DOMAINPREP** from the \i386 folder on the Windows 2003 Server CD.
4. Remove the Windows 2000 Support Tools from the Domain Controller.
5. Insert the Windows 2003 CD, click on **INSTALL WINDOWS SERVER 2003**
6. Choose **UPGRADE**, click **NEXT**
7. Accept licensing, click **NEXT**
8. If connected to the Internet, have setup download the latest patches and click **NEXT**.
9. Windows 2003 Server Compatibility Checker will run and advise you of any issues that need to be resolved before continuing.
10. Click **NEXT** to begin the upgrade

Upgrade the Atlanta Exchange Server to Windows 2003 & Exchange 2003 Server:
Since Exchange 2000 won't run on Windows 2003 [9], we must upgrade Exchange first. More information on this process is available in MSKB 822942: Considerations When You Upgrade to Exchange Server 2003 [10]

1. Insert the Exchange 2003 CD, click on **EXCHANGE DEPLOYMENT TOOLS**
2. Click on **DEPLOY THE FIRST EXCHANGE 2003 SERVER**
3. Click on **UPGRADE FROM EXCHANGE 2000 NATIVE MODE**
4. Click on Step 7: **RUN FORESTPREP NOW**
5. Click on Step 8: **RUN DOMAINPREP NOW**
6. Click on Step 9: **RUN SETUP NOW**
7. A reboot is required after Exchange 2003 setup
8. Once Exchange is upgraded, we can upgrade to Windows 2003 by following the same steps above, starting with step 4.

Install Second Atlanta Exchange Server
At this point we have a functioning, upgraded message system. But all the Internet accesible services are still running on the Atlanta Exchange server (ATLEXC1). The next step is to build and configure the second Exchange server (ATLEXC2).

1. Setup server and install hardware
2. Install Windows 2003 Server
3. Setup server IP address **192.168.0.2**

4. Join domain
5. Install Exchange 2003 Server (join existing Exchange site)
6. Per MSKB 818476: You Can Configure Either Exchange Server 2003 Standard Edition or Exchange Server 2003 Enterprise Edition as a Front-End Server [11] we need to go into the server properties in Exchange Server manage and check off **THIS IS A FRONT END SERVER**
7. Setup SMTP routing in Microsoft Exchange to accept mail for the company's domain and forward it to the internal server (ATLEXC1).
8. Finally, since there are no mailboxes available on this server, you'll want to go into Exchange System Manager dismount and then delete the information store.

Setup and Configure DMZ

The company had a Checkpoint Firewall on Windows 2000 in a single server configuration. We installed a new network card in the firewall server and hooked it up to a small 4-port switch to create our DMZ.

1. Configure new network card IP **192.168.0.1**
2. Create new network object on the Firewall, **192.168.0.1/8 subnet**
3. Create new server object on the Firewall, **ATLEXC2 192.168.0.2**
4. Setup NAT for ATLEXC2 with the same **public IP address previously being used by ATLEXC1**. This way no DNS changes are necessary.
5. Create rules to **allow incoming Internet traffic on port 25 and 443 to ATLEXC2**. We also setup a **redirect for port 80 to port 443 on ATLEXC2** for those users who may forget the HTTPS when connecting.
6. Create rules to **allow outgoing Internet traffic on ports 25 and 53 for ATLEXC2**.
7. Create rules to **allow traffic on ports 25, 80, 88, 135, 389, 3269, 6001, 6004 from ATLEXC2 to ATLEXC1**
8. Create a **drop rule to drop all other traffic from the Internet to ATLEXC2**
9. Create a **drop rule to drop all other traffic between the DMZ and Corporate LAN**

Encrypt Outlook Web Access

By default, OWA is setup and running when we installed ATLEXC2. We need to request and install our SSL certificate to encrypt OWA traffic. The company ordered a single SSL 128 bit certificate from Verisign to be installed on the server.

We were able to install Certificate Services and issue our own internal SSL Certificate to test this in the lab before the actual upgrade.

This is a fairly involved process, but we found MSKB 299875: HOW TO: Implement SSL on a Windows 2000 IIS 5.0 Computer [12] and Implementing Outlook Web Access with Exchange Server 2003 from www.MSExchange.org [13] to be big helps.

1. Open IIS, open the **Exchange** website properties
2. Click on the **Directory Security** tab and then the **Server Certificate** button to start the Web Server Certificate Wizard

3. The Wizard will walk you through preparing the Certificate request. Use the planned external address as the FQDN for the server, not it's internal name.
4. Submit Certificate Request via online service (or via email)
5. When the certificate is received (48 hours from Verisign), open IIS and the **Exchange** website properties again
6. This time, the Web Certificate Wizard will ask you if you want to **Process the Outstanding Certificate Request**, complete the Wizard to install the certificate.
7. For extra security, we enabled Forms-Based Authentication in the Exchange System Manager, per MSKB 830827: How to Use Forms Based Authentication with Outlook Web Access Clients in Exchange Server 2003 [14]

Setup RPC over HTTP on Server

The final requirement for our project was setting up encrypted remote access for users to use the Outlook 2003 client. To do this we are going to setup a new feature in Exchange 2003 called RPC over HTTP. For this section, we found MSKB 833401: How to configure RPC over HTTP in Exchange Server 2003 [15] and Configuring the Outlook 2003 RPC over HTTP Client from www.MSExchange.org [16] (for client configuration) to be very detailed.

1. On ATLEXC2, go into **Add/Remove Programs > Add/Remove Windows Components**
2. Click **Networking Services**, click **Details**, and then check off **HTTP over RPC Proxy**
3. Click **Next** and windows will install the service (the original Windows 2003 Server CD and/or a reboot may be required)
4. Then open IIS – click to expand the server name and "**default web site**"
5. Right click on the **RPC** Directory and then click **Properties**
6. Click the **Directory Security** tab, and then click **Edit** under **Authentication and access control**.
7. Click to clear the **Enable anonymous access** check box.
8. Click to select the **Basic authentication (password is sent in clear text)** check box.
9. A security-warning message appears, click **Yes**, and then click **OK**.
10. Click **Apply**
11. Click the **Directory Security** tab, and then click **Edit** under Secure communications.
12. Click to select the **Require Secure Channel (SSL)** check box and the **Require 128-bit Encryption** check box.
13. Click **OK**, click **Apply**, and then click **OK**.
14. Next, we need to make some registry changes to configure the RPC over HTTP services – open **RegEdit**
15. Browse to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\RpcProxy**
16. In the right pane, right-click **ValidPorts**, and then click **Modify**.
17. Clear the information from the **Value Data** box, and then type the following information – replacing **ServerNETBIOSName** with the RPC Proxy Server's host name and **ServerFQDN** with the RPC Proxy Server's Fully Qualified Domain Name

ServerNETBIOSName:6001;ServerFQDN:6001;ServerNetBIOSName:6004;ServerFQDN:6004

18. Next go to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters**
19. On the Edit menu, point to **New**, and then click **Multi-String Value**.
20. Name the new registry value **NSPI Interface Protocol Sequences**.
21. Right-click **NSPI Interface Protocol Sequences**, and then click **Modify**.
22. In the **Value data** box, type **ncacn_http:6004**, and then click **OK**.
23. Reboot the server for these changes to take effect.

Setup RPC over HTTP on Client (Outlook 2003)
Using the Microsoft Office Resource Kit, we customized the Outlook 2003 Deployment with the following settings for the Microsoft Exchange Service Profile. They can be viewed by going to **START > SETTINGS > CONTROL PANEL >MAIL**

1. Microsoft Exchange Server: **ATLEXC1.MURPHYBEV.LOCAL**
2. Check off **Use Cached Exchange Mode**
3. Click the **Connection** tab.
4. Click to select the **Connect to my Exchange mailbox using HTTP** check box
5. Click **Exchange Proxy Settings**.
6. Use this URL to connect to my proxy server for Exchange: **HTTPS://EMAIL.<REALDOMAIN>.COM**
7. Click **Connect using SSL only** check box.
8. Click to select the **On slow networks, connect to Exchange using HTTP first, then connect using TCP/IP** check box
9. Use this authentication when connecting to my proxy server for Exchange: click **Basic Authentication**.

Harden ATLEXC2
With the email upgrade completed, we had one final task to complete. We had to lock down ATLEXC2 since it was going to be publicly exposed on the Internet.

- Ran MS Baseline Security Analyzer v1.2, recommended and demonstrated at SANS training.
- Patched the machine to all current levels.
- Installed Anti-Virus software
- Uninstalled unnecessary IIS components
- Disabled unnecessary services
- Used Active Directory Group Policy to push the **Enterprise Client – Member Server Baseline** and the **Enterprise Client – IIS Server** Administrative Templates to set auditing, user rights, permissions, logging, and other security settings.

The use of the **High Security – Bastion Host** Administrative template is recommended for servers in the DMZ. However, running Exchange requires this server to be joined to the company's domain so the above recommendations were made.

AFTER

At the conclusion of this project the company was significantly more secure than when they started:

- DMZ for public services
- HTTPS for web based email access
- HTTPS for remote Outlook 2003 access
- Running Windows 2003 Server and IIS 6.0

For a company their size and with their Internet presence, we felt having all remote email access encrypted was pretty forward thinking. Microsoft suggests companies should consider RPC over HTTPS as an alternative to more expensive, more complex VPN solutions. [17]

We still have a large number of ports and services running and open on the Exchange sever, ATLEXC1. However, where these ports used to be open and exposed to the public Internet, they are now only exposed to the DMZ lessening the threat.

The company also engaged us in a separate project to update Outlook XP to Outlook 2003 on the company's workstations. We accomplished this with an office-by-office approach to minimize the load on the Exchange server as the new Offline Store was created on each client machine.

Users were pleased with the new GUI, Views, and Options in Outlook 2003. Specifically the Spam Filtering, and enhanced views were the most useful to users. Once Outlook 2003 was installed and configured on their laptops, users could once again use Outlook 2003 to connect from outside the Firewall remotely. Although OWA and Outlook 2003 are very similar, users still prefer to use the Outlook client whenever available.

Users were also given company approval to purchase and use wireless network cards at home and at public hotspots. Even on an unencrypted public WiFi hotspot, the SSL encryption of OWA and RPC over HTTPS would keep usernames, passwords and email messages safe.

We left the company several additional recommendations for security and performance enhancements for consideration:

- Install Microsoft Exchange Anti-Virus on ATLEXC1
- Install SMTP Gateway Anti-Virus on ATLEXC2
- ATLEXC2 should be Penetration Tested for security holes
- Reevaluate their Active Directory Domain Security Policy settings. Incorporate the enhanced AD Security Templates of Windows 2003
- Deploy SSL Encrypted mobile email access with Windows Mobile devices and Exchange Server ActiveSync
- Monitor ATLEXC2 for CPU Utilization and number of SSL Sessions. Consider possible processor upgrades or complete server upgrade if necessary.
- Monitor Firewall and ISP reports for Internet T1 usage and bandwidth consumption. Consider additional bandwidth.

Because of the small size of the organization, the overall upgrade process wasn't that difficult. However there are many details and steps involved with the upgrade, which would quickly magnify the complexity of the upgrade in a larger organization. Most of the issues we ran into could be considered speed bumps. They were quickly resolved by checking the Microsoft KB or Microsoft Newsgroups. Documentation for Windows 2003 and Exchange 2003 on the Microsoft website is through and detailed.

Additional Resources

In addition to Microsoft's site, these sites should be checked out for additional information on Exchange 2003.

Simpler-Webb Inc. Exchange 2003 FAQ
www.msexchange.org
www.outlookexchange.com

FOOTNOTES

1. Identifying company details have been changed
2. Microsoft Knowledge Base
   http://support.microsoft.com/default.aspx?scid=kb;en-us;270836&Product=exch2k
3. Symantec Security Response Center
   http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html
4. CERT.org Security Practices
   http://www.cert.org/security-improvement/practices/p075.html
5. Microsoft Windows 2003 Server White Paper
   http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/win2k/w2ktows03-2.mspx
6. Microsoft Knowledge Base
   http://support.microsoft.com/default.aspx?scid=kb;en-us;555040
7. Microsoft Knowledge Base
   http://support.microsoft.com/default.aspx?scid=kb;en-us;325379
8. Mark Ramey, Microsoft Newsgroup "microsoft.public.win2000.active_directory" 1/11/04
   http://groups.google.com/groups?hl=en&lr=&ie=UTF-8&oe=UTF-8&threadm=03f201c3d63c%24fa7f3b90%24a501280a%40phx.gbl&rnum=1&prev=/groups%3Fq%3Dinetorgpersonprevent.ldf%26hl%3Den%26lr%3D%26ie%3DUTF-8%26oe%3DUTF-8%26selm%3D03f201c3d63c%2524fa7f3b90%2524
9. SWINC.com Exchange 2003 FAQ
   http://www.swinc.com/resource/exchange2003/section4.asp
10. Microsoft Knowledge Base
    http://support.microsoft.com/default.aspx?scid=kb;en-us;822942&Product=exch2003
11. Microsoft Knowledge Base
    http://support.microsoft.com/default.aspx?scid=kb;en-us;818476&Product=exch2003
12. Microsoft Knowledge Base
    http://support.microsoft.com/default.aspx?scid=kb;EN-US;299875
13. Markus Klein, MSExchange.org "Implementing Outlook Web Access with Exchange Server 2003"
    http://msexchange.org/tutorials/OWA_Exchange_Server_2003.html
14. Microsoft Knowledge Base
    http://support.microsoft.com/default.aspx?scid=kb;en-us;830827&Product=exch2003
15. Microsoft Knowledge Base
    http://support.microsoft.com/default.aspx?scid=kb;en-us;833401&Product=exch2003
16. Thomas Shinder, MSExchange.org "Configuring the Outlook 2003 RPC over HTTP Client"
    http://msexchange.org/tutorials/outlookrpchttp.html
17. Microsoft Office 2003 Resource Kit "Configuring Outlook 2003 for RPC over HTTP
    http://www.microsoft.com/office/ork/2003/three/ch8/OutC07.htm