Is Your Email Secure?

BY JOHN E. JOHNSTON

Is there someone in your office who always seems to know the "inside scoop" on everything that goes on in your organization? Does this person also maintain your email system? While this person could possibly be psychic, chances are you may have a security exposure within your email system.

A friend of mine, a network administrator at another company, came to me recently with the following story and asked me for advice. It appears that he stumbled upon two blaring email security holes quite by accident. His shop runs Microsoft Exchange on a Windows NT server and the client workstations utilize Outlook 97 to access the Exchange server. The proxy feature of Exchange permits selected users to view other users' calendars.

Is there someone in your office who always seems to know the "inside scoop" on everything that goes on in your organization? Does this person also maintain your email system? While this person could possibly be psychic, chances are you may have a security exposure within your email system.

One day, my friend was sitting at the email administrator's workstation when an end user asked him how to view another user's calendar. He explained the concept behind proxy and proceeded to show the user how to view another user's calendar. He forgot to change the "Folder" pull-down option (shown in Figure 1) from "In Box" to "Calendar" and was quite surprised to find that he could see all of the selected user's email.

Needless to say, the user was quite surprised and quickly went to upper management, telling them that the email system was not secure. A few minutes later, my friend's number one project became "securing the email system." After further investigating the situation, he found two email security holes.

THE FIRST SECURITY HOLE

The first security exposure was caused by the type of rights granted to the Exchange administrator accounts. These rights gave the administrators ownership of every mailbox within the organization. When Exchange is set up, the rights to view other users' email is granted to the email administrators by default! To determine if your Exchange server has this same exposure, perform the following steps from your Exchange server:

- Start the Exchange Administrator program.
- Click on the Organization object to highlight it.
- Click on File > Properties.
- Click on the Permissions tab. You will see a list of users who have Exchange administrative rights.
- Highlight each user and check the "Rights" box. If the selected user has the "Mailbox Owner" right enabled, that user can potentially read all email messages on your server.
- To correct the problem, simply uncheck the "Mailbox Owner" option for each Exchange administrator. Disabling this right will not affect the Exchange administrator's job functions of setting up and managing email accounts.

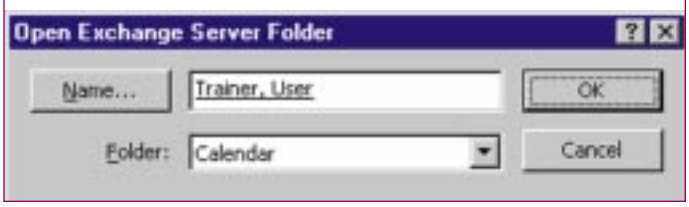
While this procedure does close the email security hole, the hole can be re-opened very easily; all the email administrator needs to do is reverse the steps above, re-instating the "Mailbox Owner" right.

THE SECOND SECURITY HOLE

Outlook 97 has an AutoArchive function. If enabled, this function automatically archives old items from your email folder(s) to an archive file. The default name for this archive file is ARCHIVE.PST. Many users choose to place their ARCHIVE.PST file on a network drive, such as their home directory. Any user who has "read" file system rights to the user's home directory can open the ARCHIVE.PST file using the Outlook 97 program. Once the archive file is opened, the intruder can view the old email documents that have been archived. The steps required to open an archive file are as follows:

- From Outlook 97, click on File > Open Special Folder > Personal Folder. A browse screen will be displayed.

Figure 1: Selecting a Calendar to View



- From the browse screen, the intruder simply browses through the network folders looking for archive files.

- After opening the archive file, the selected user's archived email messages can be read.

CLOSING THE HOLES

Closing these security holes can be difficult. Your network administrators must have sufficient rights and access to file servers in order to perform their jobs. If you lock them out, they will not be able to manage your file system(s) and file servers. You can implement the auditing facilities of your operating system, but who will implement auditing? The same people who have access to these security holes most likely. You could encrypt sensitive email using a program such as Pretty Good Privacy (PGP). PGP integrates well with Outlook 97 and is fairly simple to set up and use. The bottom line is, you have several options:

- Trust the integrity of your network and email administrators. If you are sure your administrators won't snoop around where they don't belong, you have nothing to worry about. Most network administrators that I have worked with are very respon-sible people and would not even attempt to crack an email system or read other sensitive data contained on the organization's file servers.

- Encrypt your data. While encryption can be a bit more cumbersome to use, it is the only sure way to completely secure your email.

- Have someone other than your network and email administrators set up auditing facilities. While this will not prevent unauthorized email access, it will show you who may be snooping where they shouldn't. But then, do you trust the individual(s) who set up the auditing facilities? Consider this as well.

If you have any questions, comments or ideas for future topics for this column, feel free to contact me at johnj@fast.net. ts

NaSPA member John E. Johnston is manager of technical support and communications for a major hospital in Pennsylvania. He designs and maintains cross-platform local and wide area networks utilizing NetWare, OS/2, DOS, and Windows.

