GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

SECURITY CONCERNS DURING DATA MIGRATIONS

By Robert Sanson

GSEC Practical Assignment V1.4b
Option 1 – Research on Topics in Information Security

Submitted April 14, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ABSTRACT 3

INTRODUCTION 3

BRIEF DESCRIPTION OF MICROSOFT EXCHANGE SERVER 5.5 4

BRIEF DESCRIPTION OF MICROSOFT EXCHANGE SERVER 2000 5

DESCRIPTION OF A MIGRATION SCENARIO 5

SECURITY RISK ANALYSIS OF THE MIGRATION 7

Changes to System Access Rights 7
Threat Assessment and Analysis 7
Asset Identification 7
Vulnerability Analysis 8
Risk Reduction (Mitigation) 8

Assistance from Outside Personnel 8
Threat Assessment and Analysis 8
Asset Identification 9
Vulnerability Analysis 10
Risk Reduction (Mitigation) 10

Use of Custom Software and Utilities 10
Threat Assessment and Analysis 10
Asset Identification 11
Vulnerability Analysis 11
Risk Reduction (Mitigation) 11

SECURITY CONSIDERATIONS FOR SOFTWARE MIGRATIONS 12
Evaluate the current security model and how it is used. 12
Identify and Implement the changes Needed in the security model. 12

REFERENCES 13

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

SECURITY CONCERNS DURING DATA MIGRATIONS

ABSTRACT

The urge to “get the job done” is a powerful one. When the job is a large data migration the pressure to “press on” and “do what it takes” often results in security policies being overlooked or even suspended. Data migrations are particularly susceptible to temporary security lapses. When a large amount of data must be moved from “here” to “there”, creative solutions are often used to reach the goal. Unfortunately security is often weakened or compromised. Risk increases as expertise is outsourced and customized software utilized. The more complex the migration, the more opportunities exist for security lapses.

Addressing these issues is best done by first being aware of the problem and then designing the data migration with security issues in mind. Always planning, designing and testing the migration method with a weather eye on security.

INTRODUCTION

Generally, advances in software are welcomed by users since the improvements usually add value such as enhanced security, usability, efficiency, ease of administration and so on. Organizations often upgrade their software to take advantage of these benefits although perhaps not matching the software vendors pace of software releases. The benefits of newer software come at a cost which of course must be considered.

One of the largest data migrations ever attempted is an ongoing project of the Homeland Security Department where data from 22 government agencies is to be merged cohesively and securely[1]. Security is central to this project as the data contains personal and protected information.

For this paper I will provide a context within which to examine this topic using an Email migration (Microsoft Exchange in particular) to set the background for this discussion.

Email software is some of the most used software in any organization, if not the most used. At some point the software providing email services will be upgraded.

[1]Schwartz, Karen D. “The Data Migration Challenge”. 15 December 2002. URL http://www.govexec.com/features/1202/1202managetech.htm (14 April 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

When major email software upgrades take place (beyond hotfixes and patches) there are many factors that come into play. Software and hardware changes, services/servers are often relocated geographically, specialists, vendors and contractors are often called in. When this flurry of changes is in full swing, security is one topic that is often sidelined.

This paper will examine how security is often ignored or consciously bypassed during software migrations/upgrades. Towards keeping this discussion manageable we will examine a hypothetical upgrade/migration from one Microsoft Exchange 5.5 organization to a new Microsoft Exchange 2000 AD integrated organization. This is a common upgrade path and one that provides fertile ground for our discussion.

Using this specific Microsoft Exchange upgrade scenario may appear to be narrow for a discussion on security concerns but we will see that the many security issues raised in this specific example translate well to other upgrades and data migrations.

BRIEF DESCRIPTION OF MICROSOFT EXCHANGE SERVER 5.5

Microsoft Exchange 5.5 is email server software provides email services to an organization. Clients use any version of Microsoft Outlook (usually not Outlook Express) to connect to the Exchange Server and work with their email as it is stored in the Exchange 5.5 database. Exchange 5.5 was released in 1997 and has performed admirably having a typical lifecycle of patches and service packs. Currently the recommended install should be brought to Service Pack 4 with a few additional patches.

Exchange 5.5 provides a rich environment for email and when installed to current hotfixes and patches, and managed properly provides a reliable and generally secure email environment.

Exchange 5.5 maintains its own directory of user's mailboxes and distribution lists called the Global Address List (GAL). The GAL stands on its own—synchronization with other directories is not necessary.

Access control at the server level is managed by assigning administrative and access rights to users through the user's identity as a domain member.

Access control on Exchange 5.5 is a mixed bag. For example, at the client level (access to public folders, mailboxes, calendars etc…) access control is managed by assigning access rights to users through Outlook using their mailbox identities. Mailbox ownership however, is assigned using the user's domain (user account) identity.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

BRIEF DESCRIPTION OF MICROSOFT EXCHANGE SERVER 2000

Microsoft Exchange Server 2000 is a significant upgrade to Exchange 5.5.

Exchange 2000 is email server software that provides email services to an organization. Clients use any version of Microsoft Outlook (usually not Outlook Express) to connect to the Exchange Server and work with their email as it is stored in the Exchange 2000 database. Exchange 2000 was released in October 2000 and has performed well having a typical lifecycle of patches and service packs.

A significant difference between Exchange 5.5 and Exchange 2000 is the security model used. Exchange 2000 is the first messaging system to fully integrate with the operating system; Windows 2000/Active Directory for maintaining all access controls and distribution tasks.[2]

Another significant difference between Exchange 5.5 and Exchange 2000 is in the handling of directories. While Exchange 5.5 has its self contained Global Address List (GAL), Exchange 2000 integrates fully with Windows 2000 Active Directory. Simply put, In Exchange 2000 the listing of Mailboxes, and Contacts in Outlook is provided by the network operating system (Active Directory in Windows 2000 or greater) rather than the Exchange server. Exchange 2000 handles email data; Active Directory provides the directory and security.

In Exchange 2000 access control at all levels is managed through Active Directory's security model.[3]

DESCRIPTION OF A MIGRATION SCENARIO

Microsoft Exchange Server 2000 delivers many improvements over Exchange 5.5. The changes to the back-end of Exchange are often significant enough to drive most organizations to "re-tool" their email deployment rather than doing a simple in-place upgrade.

For this example we will assume that our company's old Exchange 5.5 organization will be migrated to Exchange 2000. We will move (migrate) all the data from the old Exchange 5.5 environment onto new hardware and a new Exchange 2000 environment.

[2]Microsoft TechNet. "*The Role of Groups and Access Control Lists in MS Exchange 2000 Server Deployment*". August 2000. URL: http://www.microsoft.com/technet/prodtechnol/exchange/2000/deploy/access.mspx. (14 April 2004)

[3] Microsoft Corporation. "*Exchange 2003 Features Comparison*". 24 August 2003. URL: http://www.microsoft.com/exchange/evaluation/features/Ex_Compare.asp. (14 April 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This data migration is representative of many data migrations in that it involves moving the data from point A to point B. But, like many data migrations it's not quite that simple.

The complexity of a migration like this requires expertise in many areas. An overview of the migration steps is listed below and there are security implications throughout the process[4].

This is a very simplified look at a typical software migration. The point is that software migrations often have areas of complexity requiring elevated permissions for some tasks and outside expertise is frequently brought in to assist.

Migration Step	Security Considerations *Elevated Access*	Security Considerations *Custom Tools*
Windows 2000 Active Directory must be fully deployed	If not in place yet, this is a significant migration by itself but will not be referenced in this discussion.	
Extend Active Directory Schema to include Exchange classes and attributes	Enterprise Admin permissions are required for this step. An Enterprise Admin is the most powerful account in the domain.	Software utilities and expertise required.
Prepare the Directories (Exchange 5.5 GAL and W2K AD)	Domain Admin and Exchange Admin accounts typically used. Outside Expertise often needed.	Software utilities and expertise required.
Install first Exchange 2000 Server	Domain privileges required. Outside Expertise often needed.	
Provide for Directory Synchronization between Exchange 5.5 and Exchange 2000/AD	Domain Admin and Exchange Admin accounts typically used. Outside Expertise often needed. Foreign software often introduced at this point.	Software utilities and expertise required.

[4] Microsoft TechNet. "*Upgrading from Microsoft Exchange Server 5.5 to Microsoft Exchange 2000 Server: A Six-Step Case Scenario*". June 2002. URL: http://www.microsoft.com/technet/prodtechnol/exchange/2000/deploy/upgrademigrate/6stepap.mspx. (14 April 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Move Mailboxes, DLs and Public Folders.	Exchange Admin accounts typically used. Outside Expertise often needed. Foreign software often introduced at this point. Data at risk	Software utilities and expertise required.
Support users during transition	Exchange Admin accounts typically used. Outside Expertise often needed.	
Decommission Exchange 5.5 Systems	Exchange Admin accounts typically used. Outside Expertise often needed. Access to "old" data possible.	

Migration steps[5] and security implications.

SECURITY RISK ANALYSIS OF THE MIGRATION

CHANGES TO SYSTEM ACCESS RIGHTS

THREAT ASSESSMENT AND ANALYSIS

While performing a data migration there are often steps where significant access to systems and software is required. While this elevated access is usually temporary in nature, the exposure to risk by definition is increased.

Setting up systems and installing software require elevated or administrative rights but this is not so exceptional. Security at this point is an issue but it is a common enough occurrence that there is usually an awareness of the powerful privileges required, if not security policies concerning the very use of these administrative accounts.

It is in the environment of a technically challenging software upgrade or migration where the usual protective constraints are temporarily lifted. Extra-ordinary access is typically granted to the team working the migration.

ASSET IDENTIFICATION

Elevating access to systems for these reasons will simultaneously increase access to the data and software running on these systems. Migrations that are broad in scope typically require broader access privileges.

[5] Microsoft Corporation "*Exchange 2000 Server Deployment Best Practices and Resources*". 21 May 2001. URL: http://www.microsoft.com/exchange/techinfo/deployment/2000/AD_Best.asp (14 April 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Hardware assets at risk will include any systems that are accessible by using these elevated permissions.

Software assets at risk might be a bit harder to pin down since enterprise software often functions on a “system” of several or even many machines. The key point is whether or not the data is at risk. Data can be at risk by direct access or by damage to the data itself.

VULNERABILITY ANALYSIS

Assets are usually more vulnerable during a large software migration. Migrations and upgrades usually have points in the process where you reach the point of no return. In the case of our email migration it is at the point when the user’s mailbox data has been fully moved to the new system and the old mailbox will be deleted. Failures at these points can be very difficult to recover from.

The more access people have to systems, the more opportunities exist for mistakes, misconfiguration, mischief, etc. Hardware and Software assets are both at greater risk when more people are granted access. Especially when access is granted to people who are unfamiliar with specific or unusual configurations that might be in place.

RISK REDUCTION (MITIGATION)

There are ways to mitigate this risk. One is to, “just say no” to granting additional access. You could require that all work involving this type of access be done by partnering with an existing employee who is already trusted with this level of access.

Another way is to only grant extra-ordinary access to individual systems when absolutely necessary. And then rescind access as soon as the work is complete. This extra step involves additional work and monitoring but may be worthwhile when considering the reduction in risk it brings.

Closely monitor the work done to these systems by the people who are granted elevated access. Auditing and monitoring is an important component of risk reduction.

ASSISTANCE FROM OUTSIDE PERSONNEL

THREAT ASSESSMENT AND ANALYSIS

It is common to bring in outside help to assist with large migrations and upgrades. Outside help may come in the form of contractors, vendors, new employees or current employees who are shifted into new responsibilities.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Opening up your organization to outsiders or contractors is inherently risky for a number of reasons;

Outsiders gain knowledge of your company. For a contractor to successfully do the work that you need done, they must by definition, learn a minimum about your company's internal workings. Proprietary or otherwise, the knowledge gained from even a short stint inside your company can be used for personal gain or even malicious intent.

Outsiders are unfamiliar with your standard procedures. When outsourced help is brought in to do a specific job they are often not given a full orientation to your company. Learning your company's policies and the "way things are done" can take a significant amount of time. Even when these policies are well documented it still takes time to understand how and when they are implemented. Therefore, each outsider working in your environment increases the risk that your procedures and policies will be not be followed.

Outsiders may inappropriately access your systems. With elevated privileges, contractors may have access to more information than necessary to do their work.

For example, while testifying before the U.S. Department of Health and Human Services department regarding the use of contractors and electronic data processing, the Acting Inspector General, Michael F. Mangano noted that, "About 80 percent of the 124 weaknesses that we noted involved three types of controls: access controls… security plans…software controls".[6] This translates to physical access, security policies and software permissions.

ASSET IDENTIFICATION

When outside assistance is brought in, company assets at many levels may be at risk.

Assets such as company secrets and customer information, hardware and software systems may all be at elevated levels of risk.

The higher the level of access granted to an outsider, the broader and deeper can be the reach of the outsider.

Certainly the systems (hardware and software) that the outsider has been brought in to work on are at risk.

[6] House Energy and Commerce Committee Subcommittees on Health and Oversight and investigations Hearing. "*Testimony of Michael F. Mangano Acting Inspector General U.S Department of Health and Human Services*". 28 June 2001. URL: http://oig.hhs.gov/reading/testimony/2001/062801mm.pdf (14 April 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

System access often extends beyond just the systems that the outsider has been brought in to work on. For example if an outside contractor is granted "Domain Administrator" privileges, the level of access might be high enough to access every asset in the domain—software and hardware. You typically don't want outsiders to have this kind of access.

Access to employees and their specialized knowledge of your company is another exposure to consider.

VULNERABILITY ANALYSIS

Vulnerabilities are dependent on the level of access granted to the outsider. Projects that require outside help will typically grant elevated access to outsiders. To determine specific vulnerabilities an examination of the outsider's physical and technical access will reveal the whereabouts of vulnerabilities. Anything the outsider has access to is vulnerable to error, mishandling, damage, theft.

RISK REDUCTION (MITIGATION)

The key to reducing the risks of bringing in outside help is to control the outsider's access to your company.

Define the physical access that is appropriate to the task and put policies in place to limit outsiders' access to physical systems, buildings, and equipment.

Define the level of software permissions required for the task and put policies in place to limit outsiders' software access to just the computer systems and software necessary for their work. These restrictions can be enforced by software (permissions) and time limitations.

Simply put; Grant physical and technical access to just those company assets that are absolutely necessary to your project. And only allow access for the time the work is needed and no more[7].

USE OF CUSTOM SOFTWARE AND UTILITIES

THREAT ASSESSMENT AND ANALYSIS

Vendors in the software tools and utilities market are eager to assist with software and data migrations. They provide custom management and monitoring tools for both software, hardware and network applications. When an immediate need arises for a customized software utility vendors are often quick to create custom builds of their software for certain clients.

---

[7] Microsoft Corporation. "*Builtin and predefined groups*". 28 February 2000. URL: http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_ADgroups_9builtin_intro.htm (14 April 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

These tools are tailored to specific tasks in the migration and are often considered invaluable at simplifying and saving time and money during the migration.

However, these tools have an Achilles heel; they are often built with the priority of getting the job done. Security issues often take a back seat to the job at hand.

For example, when moving data from one email system to another there is often an interim step where the data is temporarily stored in a temporary location and then imported into the new email database. (exmerge to PST method). This is a convenient method for moving mail data but, by default the email data that was once very well protected by security policies built into Exchange, is now in a format that can be read and copied by anyone with file-level access to the temporary location.

Custom software raises risk due to its "customized" nature. This software usually hasn't had the extensive testing that major software and hardware has had. This raises the possibility that the customized software itself may cause problems.

Users of the customized software may be unfamiliar with its use, again increasing the risk of unintentional damage.

ASSET IDENTIFICATION

Wherever the custom software and utilities are used risk to the assets increases. Your company's software data is at risk of being damaged or mishandled by the customized software.

VULNERABILITY ANALYSIS

The greatest vulnerabilities are to the data or systems with which the custom software interacts. Data may be damaged and system configurations may be changed. These risks arise out of both the potential misuse of the customized software and improperly coded software.

RISK REDUCTION (MITIGATION)

The most effective way to reduce the risks of custom software is to test, test, test. It is typical practice to build a test lab[8] during the design of the migration project. This is the place to test all tools, utilities and methods that are beyond ordinary operations. This is also the place to document the use of the tools and their use with the project.

Requiring this testing will go a long way towards reducing the risks introduced by custom software and tools.

[8] Carr, Jim. "*Strategies & Issues: Blueprints for Building a Network Test Lab*". 5 April 2002. URL: http://www.networkmagazine.com/article/NMG20020401S0001 (14 April 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

SECURITY CONSIDERATIONS FOR SOFTWARE MIGRATIONS

EVALUATE THE CURRENT SECURITY MODEL AND HOW IT IS USED.

Is the current security model sufficient to handle the unique situation brought about by this software migration? Does it give clear guidance on the core security considerations of the migration such as elevated access to systems and software, the use of customized software and tools used to perform migration work, and using outside help for assistance.

IDENTIFY AND IMPLEMENT THE CHANGES NEEDED IN THE SECURITY MODEL.

After reviewing the Security Model and identifying areas of weakness, propose changes to strengthen security and adopt them.

Consider strengthening how levels of access are granted to your systems and software. Have you provided for specific time limits on these permissions?

Consider partnering outsiders with employees on migration steps where your company or its data is particularly vulnerable.

Consider implementing auditing and monitoring requirements to record all aspects of the migration with regard to these security topics.

Consider establishing clear software review and testing requirements prior to using any customized software. Require lab and production tests before approval is granted.

Consider establishing a migration security committee to serve as the security watchdog for the entire project.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

REFERENCES

[1]Schwartz, Karen D. "The Data Migration Challenge". 15 December 2002. URL http://www.govexec.com/features/1202/1202managetech.htm (14 April 2004)

[2]Microsoft TechNet. "*The Role of Groups and Access Control Lists in MS Exchange 2000 Server Deployment*". August 2000. URL: http://www.microsoft.com/technet/prodtechnol/exchange/2000/deploy/access.mspx. (14 April 2004)

[3]Microsoft Corporation. "*Exchange 2003 Features Comparison*". 24 August 2003. URL: http://www.microsoft.com/exchange/evaluation/features/Ex_Compare.asp. (14 April 2004)

[4]Microsoft TechNet. "*Upgrading from Microsoft Exchange Server 5.5 to Microsoft Exchange 2000 Server: A Six-Step Case Scenario*". June 2002. URL: http://www.microsoft.com/technet/prodtechnol/exchange/2000/deploy/upgrademigrate/6stepap.mspx.
(14 April 2004)

[5]Microsoft Corporation "*Exchange 2000 Server Deployment Best Practices and Resources*". 21 May 2001. URL: http://www.microsoft.com/exchange/techinfo/deployment/2000/AD_Best.asp (14 April 2004)

[6]House Energy and Commerce Committee Subcommittees on Health and Oversight and investigations Hearing. "*Testimony of Michael F. Mangano Acting Inspector General U.S Department of Health and Human Services*". 28 June 2001. URL: http://oig.hhs.gov/reading/testimony/2001/062801mm.pdf (14 April 2004)

[7]Microsoft Corporation. "*Builtin and predefined groups*". 28 February 2000. URL: http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_ADgroups_9builtin_intro.htm (14 April 2004)

[8]Carr, Jim. "*Strategies & Issues: Blueprints for Building a Network Test Lab*". 5 April 2002. URL: http://www.networkmagazine.com/article/NMG20020401S0001 (14 April 2004)

[9]Rosato, Rick. "*Best Practices for Applying Service Packs, Hotfixes and Security Patches.*" Microsoft TechNet. 2004.
URL:http://www.microsoft.com/technet/security/bestprac/bpsp.mspx
(14 April 2004).

© SANS Institute 2004, Author retains full rights.