Global Information Assurance Certification Paper

GroupWise 6.5 Security
Joyce Noeltner
GIAC Security Essentials Certification (GSEC) Practical Assignment, version 2.6, Option 1
August 8, 2003

"GroupWise lacks any entry whatsoever in the CERT/CC (Computer Emergency Response Team/Coordination Center) vulnerability database." [#1]

Unfortunately, this is not strictly true. There *are* CERT entries for GroupWise, albeit, for earlier versions than the one the article reviewed. [#2 and #3] Yet CERT should not be looked upon as an exclusive nor as a comprehensive listing of vulnerabilities. At the time of this writing, a search on 'groupwise' turned up only two entries at CERT while a search of the same term found 10 entries in ISS's Security Center [#4], including one filed as recently as February 2003. Again, the vulnerabilities are for earlier versions of GroupWise, but lack of a listing in CERT or any other security alert center is *not* a guarantee that any particular software is "un-hackable". It merely indicates that there just have not been enough talented people hacking at the software, seeking vulnerabilities. "Security through Obscurity" is not a strategy on which to bet the company's security. Nor one's job! This document will attempt to address GroupWise 6.5 security issues by applying the basic guiding principles that were learned during the GIAC – Security Essentials class.

- Deter
  - Create Email Security Policies
  - Place the Server Behind a Firewall
- Prevent
  - Lock Down the Server
  - Separate Operating System Volume from Data Volume
  - Restrict Access to GroupWise Directories / Resources
  - Set GroupWise Post Office Policies and Mailbox Policies
  - Lock down GroupWise WebAccess
  - Isolate Administrative Functions
  - Web Console for GroupWise Internet Agent
  - Backup's
  - Install Anti-virus and Anti-spam
  - Install Content Management
  - Enable Encryption and Personal Digital Certificates
- Detect
  - Enable Auditing
  - Install Intrusion Detection
  - Check GroupWise Logs
- Correct
  - Monitor Patches and Security Alerts
  - Document, Document, Document
  - Update And Re-Evaluate Documentation

Deter - Defense in depth

We begin by layering our defenses. Layering means to put hurdle after hurdle in front of the thing that we want to protect so that the casual predator will decide to pass us by in search of easier prey.

Create Email Security Policies

First hurdle that you should add are email security policies. “Email is increasingly being cited as primary evidence in high-profile discrimination, sexual harassment, and antitrust legal claims, according to research. According to a study conducted by the American Management Association, The ePolicy Institute and security vendor Clearswift, last year 14 per cent of firms were ordered by a court or regulatory body to produce employee email - a figure up from nine percent two years ago.” [#5] As your organization’s email administrator or as its security officer, your obligation to protect your organization from the legal liabilities that email presents is just as critical as protecting it from hackers. “..it only takes one lawsuit to severely cripple a company's financial status and morale” [#6] The best way to protect the organization against legal liabilities is to put good security policies in place. Policies are items that can be applied no matter what email package you are running.

Begin with an “Acceptable Use” policy. Just one joke in poor taste sent to the wrong recipient and suddenly your organization is in a whole heap of trouble. “Chevron recently paid out $2.2 million for sexual harassment charges after employees received an email joke listing ‘25 reasons why beer is better than women.’” [#7] Having an “Acceptable Use” policy can at least limit, if not eliminate, the damage something like that can cause. Your Acceptable Use policy should also state that your organization has the right to monitor how its resources are used. “January 2000: Nissan Motor Company. Two employees at Nissan who were fired for sending sexually explicit e-mail messages subsequently sued for unfair dismissal, claiming violation of privacy. However, Nissan won the lawsuit because it had an e-mail policy in place that prohibited the use of company owned computer systems for non-company business.“ [#8] SANS has a number of policy templates, including one for “Acceptable Use”, that you can use to create your own, changing the wording as needed to comply with the existing policies of your organization. Be aware: you need to do more than merely publish your “Acceptable Use” policy in your employee handbook. Retain a copy of the Acceptable Use policy signed by each employee with a statement that they have read and understood the policy. Then if an employee is fired for violating the Acceptable Use policy, you have greatly reduced their chances of successfully suing your organization for “wrongful termination” because he/she “was not aware of the policy”.

Also consider adding a disclaimer to the end of every message. An email message has the same weight as something sent on company letterhead. Unfortunately, email tends to lend itself towards casual conversation. "'Off-the-cuff, casual email conversations among employees are exactly the type of messages that tend to trigger lawsuits, arm prosecutors with damaging evidence, and provide the media with embarrassing real-life disaster stories,' said [Nancy] Flynn [executive director of The ePolicy Institute]." [#5] "Defamation, unintended contract formation, misdirected emails confidentiality, legal privilege, infringement of copyright and other wrongful acts, viruses, sexual and racial discrimination, harassment are a few reasons for considering disclaimers." [#9] Think about each of these, is it a situation that could happen at your organization? Search for disclaimers that address that particular situation and use that wording or write your own.

Also give a lot of consideration to an email retention policy. "The research found that, in spite of growing scrutiny from courts and regulators, most employers are doing a poor job of managing email business records and are unprepared for the likelihood of email discovery. Only 34 per cent of employers currently have a written email retention and deletion policy in place, the same figure reported in 2001, 12 months before five Wall Street brokerages were fined $8.3m (£4.9m) for failing to retain emails." [#5] So now you're a true believer and you want to create an email retention policy for your organization. "One of the most frequently asked questions is: how long do you need to store email? As with paper, there is a need to retain this information for a set period, but the exact time still remains vague. 'The Data Protection Act [DPA] says that data should be kept for as long as is necessary for the purpose it was obtained,' explained James Mullock, a lawyer with law firm Osborne Clarke. And you can't get much more vague than that." [#10] Unfortunately, the situation is similar in the USA and elsewhere because case laws on the subject are still evolving. In other words, there are no easy answers here. SANS has a template for email retention that you can use as a guideline. [#11] Also review your organization's current paper document retention policies and/or the document retention policies of other organizations in your industry to help you to create your email retention policy. And err on the conservative side.

Of course, you also have to enforce any policies you make. ".. according to the SHRM [Society for Human Resource Management], slightly more than half of their members (52%), had written email policies, and of these, only a quarter are actually enforcing them -- which can be as expensive as not having a policy at all." [#7] Not only should you install software to implement your security policies but you need to create, *and follow,* procedures to enforce your policies.

Now let's consider the more technical aspects of protecting your GroupWise email server and look at the next set of hurdles we should install.

Place the Server Behind a Firewall

Most organizations require a way to send and receive email across the internet. If the organization has more than one mail server, usually all internet-bound messages are funneled to one particular server to handle the job of sending mail to external addresses. The same server is usually used to receive all inward-bound mail from the internet. For those mail servers that need to be connected to the internet, one of the best technical defenses you can give it is to place the server behind a firewall and restrict external access to it to only specific ports.

- Port 25 - smtp
- Ports 80 – http, 389 – LDAP and 636 – SSL for LDAP but only if you intend to use GroupWise Web Access
- Ports 110 - POP3 and 143 - IMAP but only if you intend to allow POP3 access

You do not have to use the same server for external smtp traffic, POP3 and/or GroupWise Web Access, so you may want to consider having separate servers handle those duties.

A firewall is not the be-all, end-all, cure-all, but it's a good start.

Prevent

This will be the largest section. Recall the old saying: "An ounce of prevention is worth a pound of cure". You'll do yourself the greatest good by spending the most effort here.

Lock Down the Server

The next hurdle we'll put up is the security of the server itself. Think about its security as just a plain-jane server and what would need to be done in that respect. (We'll get into tightening its security as a GroupWise server later.) There are a number of great references available that give specific advice for locking down a generic NetWare NDS server.

- Securing Novell NetWare 6 [#12]
- NetWare 4 and 5 Security Guide and Checklist [#13]
- Novell's documentation on NetWare 5.1 Security [#14]

Some GroupWise server services (aka "GroupWise Agent") can also run on a Windows NT 4 or Windows 2000 server and there are excellent guides for locking down those operating systems as well.

- Microsoft Solution for Securing Windows 2000 Server [#15]
- Maintain Security with Windows NT Server 4.0 [#16]

Keep in mind, when you run GroupWise Agent on a Windows server, the GroupWise Agent needs a valid NDS account that it can use to connect to the GroupWise domain. That means that running GroupWise Agent on a Windows

server represents a slightly greater security hazard to your network if someone manages to breach the Windows server.

Separate Operating System Volumes From Data Volumes

No matter what operating system you use, it's a good rule of thumb to place the operating system and it's files on a volume or drive that is isolated from user data. If your NetWare server's SYS volume runs out of space, to be blunt, your server *will* abend and you'll have a fight on your hands trying to get it back to normal. Yet users tend to email a lot of attachments to each other; word processing documents, spreadsheets, pictures, overhead presentations, what have you. Attachments, of course, need a lot of space on your server which means you're looking at a potential conflict. So save yourself a lot of heartache and grief by making sure the data directories for GroupWise are on a different volume than SYS.

Restrict Access to GroupWise Directories and Objects

During the installation of GroupWise, the installer asks where it should place the GroupWise client software. A directory with installation software does not grow as quickly as a directory holding user data but you still may want to avoid placing the files on your SYS volume. The GroupWise installer usually suggests creating a subdirectory named "Grpwise\software" under PUBLIC on the server's SYS volume. In a default install of NetWare, users are given only READ and FILE SCAN rights to SYS:PUBLIC. That also happens to be all the rights that your users require in order to access and use the GroupWise client installation software. So if you place the files on a different volume on the server, be sure to set the rights for the software install directory to only READ and FILE SCAN.

You may also want to stop users from arbitrarily installing the GroupWise client or other software on their workstation, so when you set the rights for the software directory, consider giving rights only to specific OU's, groups or users instead of to the "PUBLIC" group.

Next, let's consider the directories that hold the GroupWise database files. Unless you are going to allow your GroupWise clients to use "Direct Access" instead of "Client/Server Access", users do not need rights to the database directories. A default installation of GroupWise uses "Client/Server Access" which is much more secure. If, however, you decide you want your GroupWise clients to use "Direct Access", follow the suggestions of the following page: "GroupWise 6.5 – Security – File System Rights", http://www.novell.com/documentation/lg/gw65/gw65_security/data/akg0pe3.html [#17]

Next, let's consider NDS or eDirectory rights. GroupWise users need rights to the GroupWise NDS (or eDirectory) objects so they can look up other users in the

address book, etc.. Unless you change the defaults, when you create a new GroupWise account, the account will automatically receive the correct eDirectory rights it needs. There may be situations where you want to disable the automatic settings and, instead, set those rights by hand but it's generally not recommended. If you decide that's what you want to do, follow the instructions found here: "GroupWise 6.5 – Security – eDirectory Rights", http://www.novell.com/documentation/lg/gw65/gw65_security/data/akfzfgh.html [#18]

Set GroupWise Post Office and Mailbox Policies

After installing GroupWise, you'll want to enabled "Intruder Detection" on the Post Office. You also need to decide what type of password requirements you want to set on your GroupWise mailboxes. If the post office is set for "low" security, anyone can open anyone else's mailbox. Obviously we don't want that. So we want to set post office security to "high".

- Enable Intruder Detection: Open ConsoleOne. Find the Post Office object and double click it to open its "Properties" window. Under the "GroupWise" tab, select "Client Access Settings". Place a checkmark in the box next to "Enable Intruder Detection". Review the default detection settings, reconfigure as necessary to best fit your environment. Click "OK" to save your changes. (See Figure 1.)

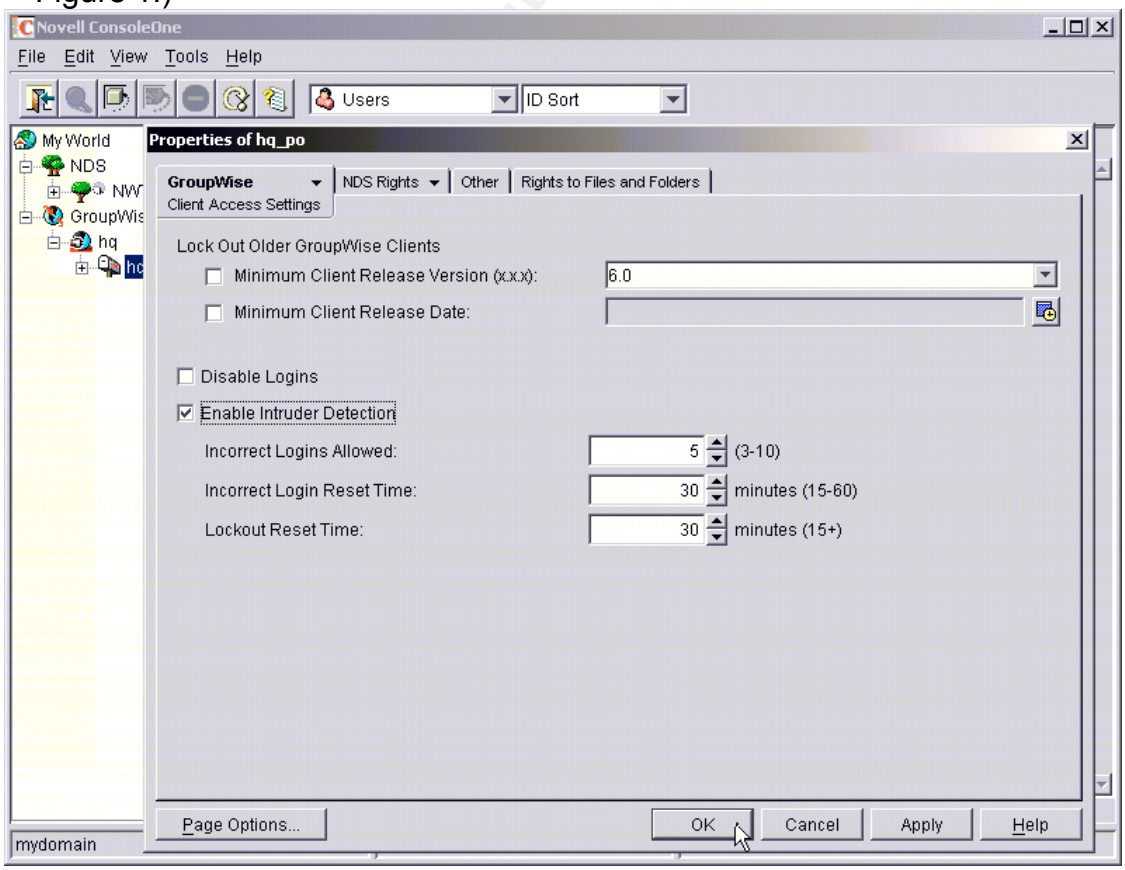

Figure 1 - Enable Intruder Detection on the Post Office

- Set Post Office Security: Open ConsoleOne. Find the Post Office object and double click it to open its "Properties" window. Under the "GroupWise" tab, select "Security". Make sure to set the Security Level to "High" then choose the authentication you will allow: eDirectory (ie, the user must be successfully logged into NDS) and/or LDAP. See figure 2 below. (Note: users themselves can add yet another layer of security by placing a password on their mailbox.)

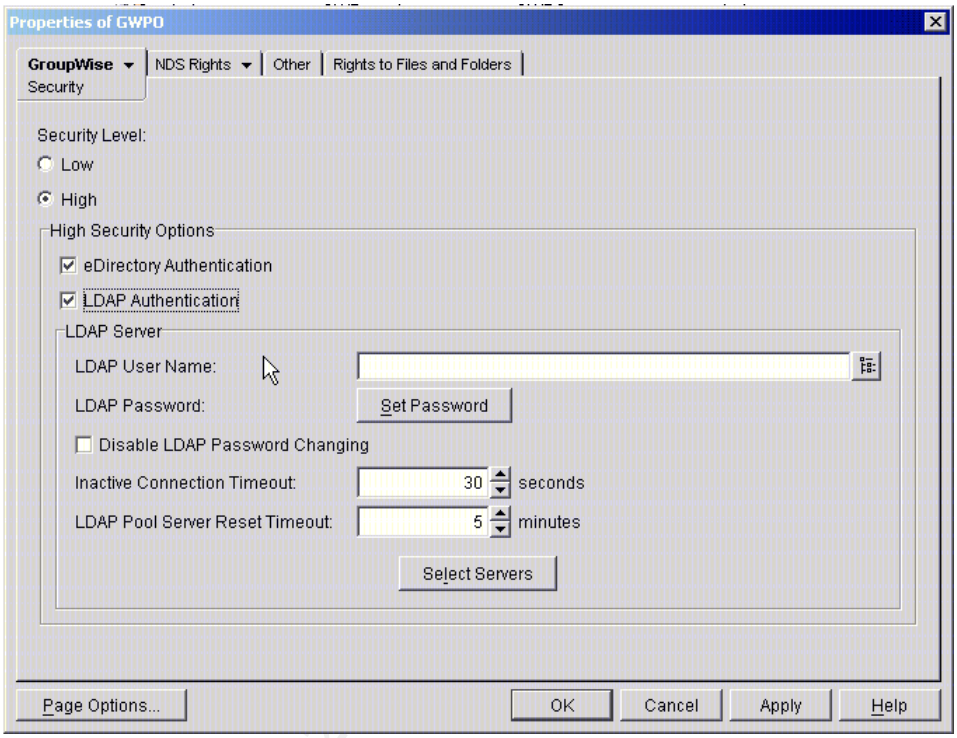

Figure 2 - Post Office Security Level

Lock Down GroupWise WebAccess

The good news is that GroupWise WebAccess (ie, the server program that allows users to access their mailbox via a web browser) enables "Intruder Detection" by default. Bad news is that we cannot make changes to the "Intruder Detection" settings. However, there are other restrictions that we can apply to further enhance WebAccess security. For instance, some of our fellow GroupWise administrators have sent in suggestions to "Novell GroupWise Cool Solutions" for forcing GroupWise WebAccess to accept *only* an SSL login. The first suggestion uses javascript. The second, does not.

- "How to Force SSL Login on GroupWise WebAccess" http://www.novell.com/coolsolutions/gwmag/features/tips/t_tip_force_ssl_login_gw.html [#19]
- "SSL Login on GroupWise WebAccess" http://www.novell.com/coolsolutions/gwmag/features/tips/t_tip_force_ssl_webaccess_login_gw.html [#20]

Web Console for GroupWise Internet Agent

The Web Console for GroupWise Internet Agent allows us to see smtp traffic statistics and other statistical information about our server through a web browser. However, Novell recommends that, if you use the Web Console, you should give it an arbitrary user name and password. In other words, don't use an NDS or eDirectory user name or password as that is viewed as a potential security risk.

LDAP authentication and Bind

If you allow your users to authenticate through an LDAP server, be sure to enable it using "bind" instead of "compare". "Bind" enforces LDAP password policies (grace logins, intruder lockout, etc.) while "compare" merely checks if the password given by the user requesting to login matches their password in the LDAP directory. In other words, if you use "compare", someone could try brute forcing the password because it's not checking if the account is locked after x-number of bad tries.

Isolate Administrative Functions

Once your NDS tree's schema has been extended to add GroupWise elements, there's no reason that the person who does the day-to-day administration of GroupWise to be 'root' equivalent. Separating "GroupWise Only" administration tasks from NDS administration tasks limits the exposure of your network to potential damage if the GroupWise Admin account is ever compromised. There are several different types of GroupWise administrators, however. Refer to the links below. With the first link, read about each type of administrator and what that administrator has rights to do. The second link has the steps to follow to set it up.

- "GroupWise 6.5 – Security – GroupWise Administrator Rights – Assigning Rights Based on Administrative Responsibilities", http://www.novell.com/documentation/lg/gw65/gw65_security/data/a4i1mi3.html [#21]
- "GroupWise 6.5 – Security – GroupWise Administrator Rights", http://www.novell.com/documentation/lg/gw65/gw65_security/data/ak9e6f4.html [#22]

Backup's

You need to decide what software to use, what needs to be backed up and how often should backup's take place. "How often" will depend on how quickly you want to be able to recover an object and how much risk you're willing to take. Document your backup and restoration steps: how to restore the domain, a post office, a single user account, a mailbox item, etc.

- "Restore a Domain" – http://www.novell.com/documentation/lg/gw65/gw65_admin/data/a488bd9.html [#23]
- "Restore a Post Office" - http://www.novell.com/documentation/lg/gw65/gw65_admin/data/a488bft.html [#24]
- "Recovering Deleted GroupWise Accounts in GroupWise 6.5", http://www.novell.com/coolsolutions/gwmag/features/tips/t_recover_deleted_account_utility_gw.html [#25]
- "Restore Deleted Mailbox Items", http://www.novell.com/documentation/lg/gw65/gw65_admin/data/abcggai.html [#26]

Since GroupWise is, at its heart and soul, a database, be sure to choose a backup product that's certified to work with GroupWise. Some third-party backup products:

- Syncsort Backup Express – http://www.syncsort.com [#27]
- Veritas Backup Exec – http://www.veritas.com and http://www.veritas.com/products/category/ProductKeywordDetail.jhtml?productKeywordId=190&productId=benw [#28]
- Computer Associates' ARCserve Backup Agent for GroupWise – http://www.ca.com and http://www3.ca.com/Solutions/ProductOption.asp?ID=2755 [#29]

Anti-virus and Anti-Spam

It now goes without saying that an email system needs anti-virus protection. Just because someone has not yet created a virus that specifically targets the GroupWise client, that does not mean it can never happen. And, of course, users can still become infected if they launch a virus-infected attachment. With the rising tide of unwanted spam, email administrators are now facing another challenge. Fortunately, many makers of anti-virus software also offer anti-spam products.

Third-Party Anti-Virus and/or Anti-Spam Products:

- AppRiver's, Spam Filtering Service - http://www.appriver.com [#30]
- Beginfinite's GWAVA – http://www.beginfinite.com [#31]
- Caledonia's Iris PureMail – http://www.caledonia.net/iris.html [#32]
- CipherTrust's IronMail – http://www.ciphertrust.com/ironmail [#33]
- OpenHand's Guinevere – http://www.openhandhome.com [#34]
- IntelliReach's MessageScreen – http://www.intellireach.com [#35]
- MailWise – http://www.mailwise.com [#36]
- Omni Technology Solutions Inc.'s GEE Whiz – http://www.omni-ts.com [#37]
- The Messaging Architects' GWGuardian- http://www.gwtools.com [#38]
- SurfControl – http://www.surfcontrol.com [#39]

Can't quite convince management to spring for anti-spam-ware? Have them consider this: "'Just as an employer has a duty to protect from patrons and other people--like the (delivery) guy who fondles a secretary--there's a good theory saying a company has a duty to filter (offensive e-mail) even if the employees are being harassed entirely from far outside the company walls,' [Eugene] Volokh [a professor of law at UCLA] said. 'If the employer is reasonably capable of filtering the material, and if it doesn't do that, it would be held liable.'" [#40] In other words, it's up to the employer to protect their employees.

- "Email, Adult Content, and Employment Law: Reducing Corporate Liability With Filtering and Policy Tools", http://www.postini.com/upe/Legal_Liability_White_paper.pdf [#41]
- "Client Alert – Third Circuit and New Jersy Appellate Division Decisions Expand Employers' Potential Vicarious Liability for Workplace Harassment by Supervisors", http://www.proskauer.com/news_publications/client_alerts/content/2003_04_00_g/get_data?k=PDF [#42]
- "Another Reason to Fight Spam", http://www.nwfusion.com/newsletters/gwm/2002/01644269.html [#43]
- "Strategies for Winning the War on Spam", http://www.businessweek.com/technology/content/aug2002/tc20020820_1318.htm [#44]

Content management

Content Management is about protecting your organization from information leakage. Publish policies against sending sensitive, proprietary or confidential information. Audit messages to ensure that such information is not released. Many anti-spam products use a scoring system to judge if a message is spam or not. They look at the content of a message, hunt for key words or phrases. A secondary use for your anti-spam software could be for auditing content. There are, of course, content management products too. Another highly vexing issue with no easy answers is whether or not to allow users to store their mail on the server or on their local workstation. If you allow users to store their mail on their local computers, then you have to consider the security of the workstation. That, of course, includes laptops which greatly increases the danger your organization faces. Add to this mix the fact that GroupWise 6.5 includes support for PDA's and you're looking at a highly dangerous potential for information leak. A Content Management product can at least help you to identify those users who have potentially risky information in their mailboxes.

Suppose you decide that the potential risk of information leakage is too great and want to create a policy that states users cannot store mail on their local computer/laptop/PDA? You'll fight a major battle to get your policy in place. Here's where content management software can help you, once again. You can show your organization's management precisely the danger of information

leakage that organization faces if they allow users to store mail on their laptops and/or PDA's. You'll probably get at least a few converts to your side.

Encryption and Personal digital certificates

There are times, however, when proprietary, confidential or sensitive information *must* be sent to recipients who are outside of your organization. We can allow this if we give our users the ability to send and receive those messages in a secure manner. This is explained in a recent Novell Appnote: "Sending Secure and Encrypted Messages with Groupwise 6.5" [#45] If your users need to send sensitive information, be sure to include in your security policies a policy for sending encrypted messages. The policy should cover the minimum acceptable encryption level, encryption software, what is meant by "sensitive information", etc.. Again, there are sample policies at SANS that you can use for a guide. Those policies can be found here: "Acceptable Encryption Policy", http://www.sans.org/resources/policies/Acceptable_Encryption_Policy.pdf [#46] and "Information Sensitivity Policy", http://www.sans.org/resources/policies/Information_Sensitivity_Policy.pdf [#47]

Detect

Suppose, despite all the hurdles we've put up, someone still manages to compromise our server. How will we know? That's the idea behind "Detect". Periodically check for telltale signs or putting tracking in place so we can tell what happened and when it happened.

Enable Auditing

NetWare has had built-in auditing for a number of generations.

- "NetWare 6 – Auditing the Network", http://www.novell.com/documentation/lg/nw6p/auditenu/data/a2q3x2v.html [#48]
- "NetWare 5.1 – Auditing the Network", http://www.novell.com/documentation/lg/nw51/auditenu/data/a2q3x2v.html [#49]
- "NetWare 4.2 – Auditing the Network", http://www.novell.com/documentation/lg/nw42/auditenu/data/a7ppqip.html [#50]

Even GroupWise has "intruder detection". But you may want something more robust and flexible, check out these products.

- Novell's Nsure Audit, http://www.novell.com/products/nsureaudit/ [#51]
- Novell's Advanced Audit Service, http://www.novell.com/documentation/lg/nw6p/naas_enu/data/a4fe5v6.html [#52]

- Symantec Enterprise Security Manager, http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=45 [#53]
- Symantec Intruder Alert, http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=171 [#54]
- Blue Lance's LT Auditor+, http://www.bluelance.com [#55]

Check GroupWise Logs

Once again, we have one of our fellow GroupWise administrators to thank for submitting a nice tool for us. In this case, the GWIA Log Utility reads the GroupWise Internet Gateway logs so you can get a high level overview of what's been happening. According to Jim MacLachlan (the author of GWIA Log), "You will get a rough idea of the daily traffic and can keep an eye on the email addresses passing through it. [..] It has also alerted us to employees who are abusing their Internet email usage. One hourly employee wrote 700 emails over the course of the month and their job required little to no Internet email." You can find it here: http://www.novell.com/coolsolutions/tools/1457.html [#56]

Correct

Our focus here is "how do we fix things"? This can cover a variety of aspects from fixing things after a security compromise or getting ourselves online again after a hardware failure. Although this comes near the end of our document, much of it entails planning ahead.

Monitor Patches and Security Alerts

Periodically check for new patches, both for GroupWise and for the server operating system it's running on. Also check for security alerts.

- http://support.novell.com - Novell's support site, including their online Knowledgebase and the "Patches and Fixes" site [#57]
- http://support.novell.com/filefinder/security/ - Novell security alerts [#58]
- http://www.novell.com/coolsolutions/gwmag/ - Novell GroupWise Cool Solutions [#59]
- http://www.sans.org/newsletters/ - SANS' Computer Security Newsletters and Digests [#60]
- http://www.kb.cert.org - CERT Coordination Center Knowledgebase [#61]
- http://www.iss.net/security_center/ - ISS Security Center [#62]

Document, Document, Document!

Document your Disaster Recovery Procedures. Ask yourself: "What would I need to do to get the server running in the shortest amount of time: if I need to replace hardware; if I needed to restore on different hardware; etc..?" Create Business Continuity Plans: "What should we do to keep things flowing during and after a

disaster?" And document your procedures for handling a Security Incident: "Who must be notified internally? Who decides if we'll pursue litigation? If we do, what proof will we need to make our case? How do we juggle gathering the proof we need for the case *and* the high pressure need to get the server back online in a reasonable time period? How do we analyze what was breached to find out what happened and how to prevent it from happening again?" Documentation is a boring job but force yourself, make time to do it. You're going to find yourself a tad too distracted while you're fighting the fires of a disaster to properly think things through the way you should. Good documentation can give you an idea of which direction you need to jump next. *Always* get management's approval for the steps outlined by your Security Incident Handling document *before* an incident! Try to get it approved from as high up in your organization as you can. It's funny how management's expectations of what *should* be done are completely different while a disaster is in progress vs. after it's over. Use your approved "Security Incident Handling Procedures" document as your guide for gathering evidence with a view towards pursuing litigation. If your organization's upper management starts pushing to "get things back the way they were ASAP!", you can remind them again that to do so means that they are very likely destroying any chance at a successful court case. If that's still what they want, at least you've dotted your I's, crossed your T's and covered .. what needs to be covered.

Update And Re-Evaluate Documentation

Update your documentation on a regular basis to keep it current. Be sure to include in your Disaster Recovery documentation all the latest patches or hot-fixes that have been applied or other changes that have taken place since the last revision. Re-evaluate your Security Incident Handling Procedures document after a breach or a disaster to add "lessons learned". Also re-evaluate your other internal procedures and policies. Are there changes that need to be made there? Hindsight, as they say, is 20/20. Now is when you take that clear-sightedness and incorporate it into your documentation.

References

1. "Novell Readies a Challenger for Notes, Exchange", by P. J. Connolly, May 23, 2003, InfoWorld, URL http://www.infoworld.com/article/03/05/23/21TCgroupwise_1.html?s=tc

2. CERT Vulnerability Notes VU341539, "Novell GroupWise Server Web-Based Front-End Does Not Adequately Validate User Input Thereby Allowing Directory Traversal", Published September 27, 2002, CERT Coordination Center, URL http://www.kb.cert.org/vuls/id/341539, which affects GroupWise 5.5 Enhancement Pack and GroupWise 6

3. CERT Vulnerability Notes VU726891, "Novell GroupWise Contains Protocol Implementation Vulnerability Allowing Email To Be Viewed By Unauthorized User", Published January 31, 2002, CERT Coordination Center, URL http://www.kb.cert.org/vuls/id/726891, which affects GroupWise 5.5 Enhancement Pack through Service Pack 3 and GroupWise 6.

4. ISS's Security Center http://www.iss.net/security_center/

5. "Firms at Risk on Email Legal Liability", by Robert Jaques, June 18, 2003, Network News, URL http://www.networknews.co.uk/News/1141688

6. "Five Ways You Can Protect Your Company From Email Usage Lawsuits", by Victor Woodward, Domino Power Magazine, URL http://www.dominopower.com/issues/issue199811/fiveways001.html, http://www.dominopower.com/issues/issue199811/fiveways002.html and http://www.dominopower.com/issues/issue199811/fiveways003.html

7. "It's the email, stupid!", by Victor Woodward, Domino Power Magazine, URL http://www.dominopower.com/issuesprint/issue199812/legal.html

8. "Legal Liability Issues with Email and the Web", by Julie Spencer, March 22, 2003, Brainbox, URL http://www.brainbox.com.au/brainbox/home.nsf/0/FA74F23822ADA289CA256CF0000328EE?opendocument

9. "Email Disclaimers", by Alan Davidson, December 2002, CyberLaw, URL http://www.uq.edu.au/davidson/cyberlaw/december2002.html

10. "Email Retention Rules Must Be Spelled Out", by Chris Green, July 4, 2003, Computing, URL http://www.computing.co.uk/Features/1142048

11. "Email Retention Policy", SANS, URL http://www.sans.org/resources/policies/email_retention.pdf

12. "Securing Novell NetWare 6", by Darren Mattila, September 4, 2002, SANS Reading Room, URL http://www.sans.org/rr/paper.php?id=908

13. "NetWare 4 and 5 Security Guide and Checklist", by Mark Sanderson, September 5, 2001, SANS Reading Room, URL http://www.sans.org/rr/paper.php?id=248

14. "NetWare 5.1 – NetWare Server Security", Novell, URL http://www.novell.com/documentation/lg/nw51/ssec_enu/data/hjc2z4tu.html

15. “Microsoft Solution - Windows 2000 Server Security Checklist”, Microsoft, URL http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/Default.asp

16. “Maintain Security with Windows NT Server 4.0”, Microsoft, URL http://www.microsoft.com/ntserver/security/default.asp

17. “GroupWise 6.5 – Security – File System Rights”, Novell, URL http://www.novell.com/documentation/lg/gw65/gw65_security/data/akg0pe3.html

18. “GroupWise 6.5 – Security – eDirectory Rights”, Novell, URL http://www.novell.com/documentation/lg/gw65/gw65_security/data/akfzfqh.html

19. “How to Force SSL Login on GroupWise WebAccess”, GroupWise Cool Solution submitted by Robert Stout, November 27, 2002, Novell, URL http://www.novell.com/coolsolutions/gwmag/features/tips/t_tip_force_ssl_login_gw.html

20. “SSL Login on GroupWise WebAccess”, GroupWise Cool Solution submitted by Charles Ransom, February 5, 2003, Novell, URL http://www.novell.com/coolsolutions/gwmag/features/tips/t_tip_force_ssl_webaccess_login_gw.html

21. “GroupWise 6.5 – Security – GroupWise Administrator Rights – Assigning Rights Based on Administrative Responsibilities”, Novell, URL http://www.novell.com/documentation/lg/gw65/gw65_security/data/a4i1mi3.html

22. “GroupWise 6.5 – Security – GroupWise Administrator Rights”, Novell, URL http://www.novell.com/documentation/lg/gw65/gw65_security/data/ak9e6f4.html

23. “GroupWise 6.5 – GroupWise 6.5 Administration Guide – Databases – Restoring GroupWise Databases From Backup - Restoring a Domain”, Novell, URL http://www.novell.com/documentation/lg/gw65/gw65_admin/data/a488bd9.html

24. “GroupWise 6.5 – GroupWise 6.5 Administration Guide – Databases – Restoring GroupWise Databases From Backup - Restoring a Post Office”, Novell, URL http://www.novell.com/documentation/lg/gw65/gw65_admin/data/a488bft.html

25. “Recovering Deleted GroupWise Accounts in GroupWise 6.5”, May 29, 2003, Novell, URL http://www.novell.com/coolsolutions/gwmag/features/tips/t_recover_deleted_account_utility_gw.html

26. “GroupWise 6.5 – GroupWise 6.5 Administration Guide – Restoring GroupWise Databases from Backup - Restore Deleted Mailbox Items”, Novell, URL http://www.novell.com/documentation/lg/gw65/gw65_admin/data/abcggai.html

27. Syncsort Backup Express, URL http://www.syncsort.com and http://www.syncsort.com/bex/infobex.htm

28. Veritas' Backup Exec, URL http://www.veritas.com and http://www.veritas.com/products/category/ProductKeywordDetail.jhtml?productKeywordId=190&productId=benw

29. Computer Associates' BrightStor, ARCserve Backup Agent for GroupWise, URL http://www.ca.com and http://www3.ca.com/Solutions/ProductOption.asp?ID=2755

30. AppRiver's Spam Filtering Service, URL http://www.appriver.com

31. Beginfinite's GWAVA, URL http://www.beginfinite.com

32. Caledonia's Iris PureMail, URL http://www.caledonia.net/iris.html

33. CipherTrust's IronMail, URL http://www.ciphertrust.com/ironmail

34. OpenHand's Guinevere, URL http://www.openhandhome.com

35. IntelliReach's MessageScreen, URL http://www.intellireach.com

36. MailWise, URL http://www.mailwise.com

37. Omni Technology Solutions Inc.'s GEE Whiz, URL http://www.omni-ts.com

38. The Messaging Architects' GWGuardian, URL http://www.gwtools.com

39. SurfControl, URL http://www.surfcontrol.com

40. "Porn Spam: Are Employers Liable?", by Declan McCullagh, April 7, 2003, ZD Net, URL http://zdnet.com.com/2100-1105-995658.html

41. "Email, Adult Content, and Employment Law: Reducing Corporate Liability With Filtering and Policy Tools", Michael R. Overly, Esq., Foley & Lardner, Postini Corp, URL http://www.postini.com/upe/Legal_Liability_White_paper.pdf

42. "Client Alert – Third Circuit and New Jersey Appellate Division Decisions Expand Employers' Potential Vicarious Liability for Workplace Harassment by Supervisors", April 2003, Proskauser Rose, URL http://www.proskauer.com/news_publications/client_alerts/content/2003_04_00_g/get_data?k=PDF

43. "Another Reason to Fight Spam", by Michael Osterman, Network World Fusion, November 25, 2002, URL http://www.nwfusion.com/newsletters/gwm/2002/01644269.html

44. "Strategies for Winning the War on Spam", by Alex Salkever, August 20, 2002, Business Week Online, URL http://www.businessweek.com/technology/content/aug2002/tc20020820_1318.htm

45. "Sending Secure and Encrypted Messages with Groupwise 6.5", By Tay Kratzer, Novell AppNotes, URL http://developer.novell.com/research/appnotes/2003/may/02/a030502.pdf

46. "Acceptable Encryption Policy", SANS, URL http://www.sans.org/resources/policies/Acceptable_Encryption_Policy.pdf

47. "Information Sensitivity Policy", SANS, URL http://www.sans.org/resources/policies/Information_Sensitivity_Policy.pdf

48. "NetWare 6 – Auditing the Network", Novell, URL http://www.novell.com/documentation/lg/nw6p/auditenu/data/a2q3x2v.html

49. "NetWare 5.1 – Auditing the Network", Novell, URL http://www.novell.com/documentation/lg/nw51/auditenu/data/a2q3x2v.html

50. "NetWare 4.2 – Auditing the Network", Novell, URL http://www.novell.com/documentation/lg/nw42/auditenu/data/a7ppqip.html

51. Novell's Nsure Audit, URL http://www.novell.com/products/nsureaudit/

52. Novell's Advanced Audit Service, URL http://www.novell.com/documentation/lg/nw6p/naas_enu/data/a4fe5v6.html

53. Symantec Enterprise Security Manager, URL http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=45

54. Symantec Intruder Alert, URL http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=171

55. Blue Lance's LT Auditor+, URL http://www.bluelance.com

56. GWIA Log Utility, GroupWise Cool Solution submitted by Jim MacLachlan, Novell, URL http://www.novell.com/coolsolutions/tools/1457.html

57. http://support.novell.com - Novell's support site, including the online Knowledgebase and the "Patches and Fixes" site

58. http://support.novell.com/filefinder/security/ - Novell security alerts

59. http://www.novell.com/coolsolutions/gwmag/ - Novell GroupWise Cool Solutions

60. http://www.sans.org/newsletters/ - SANS' Computer Security Newsletters and Digests

61. http://www.kb.cert.org - CERT Coordination Center Knowledgebase

62. http://www.iss.net/security_center/ - ISS Security Center

All links were current as of August 8, 2003.