Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Novell Small Business Suite Security Recommendations

The Novell Small Business Suite is a powerful tool for a small business, at a low price. Because small businesses have limited budgets, they have limited capability to install, configure, patch and maintain their servers. Because of the technical complexity of such products, it can be easy for security holes to be found and taken advantage of without a small business being aware. Novell has a reputation for strong security. But, since converting their product to become TCP/IP based, it has many potential security risks...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

Novell Small Business Suite Security Recommendations

Scott T. Stone, MCNE, MCSE, SSCP

October 31st, 2003

GIAC Security Essentials Certification (GSEC) Practical Assignment

Version 1.4b

Option #1

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

The Novell Small Business Suite is a powerful tool for a small business, at a low price. Because small businesses have limited budgets, they have limited capability to install, configure, patch and maintain their servers. Because of the technical complexity of such products, it can be easy for security holes to be found and taken advantage of without a small business being aware.

Novell has a reputation for strong security. But, since converting their product to become TCP/IP based, it has many potential security risks not yet recognized.

Introduction

The small business market in American business could be characterized by those businesses that have a small number of employees, lean budgets, and reduced access to technical resources.

In the year 2000, of the approximately 5.6 million businesses in the U.S., more than 4.8 million, or 98%, had fewer than 100 employees; 78% had less than 10 employees. [CENSUS]

The small business market requires computers, and is being marketed to by large companies offering technically complex packaged products that have inherent security features -- and vulnerabilities -- that can potentially impact people outside of their businesses. Also, because of the nature of the small business market, these companies have minimal budgets to install, setup, maintain, update and patch these complex products. "Small businesses often don't have the resources to manage their own IT needs. They often lack the financial means to constantly maintain or update their systems. More than 45% of small business owners feel that technology is inhibiting--not contributing to--their growth." [RILEY].

Companies such as Microsoft and Novell have business groups within their organizations that market affordable products directly to small businesses. In particular, Microsoft has a Small Business Server product that has grown in scope over the past few years, with SBS 4.5, and then SBS 2000, and now SBS 2003. [MICROSOFT]. Novell also has a Small Business Suite 6.5 as their latest product focused on this market. [NOVELL1].

Both are combined packages, or suites, which include many of their individual products, bundled together. A limit on total user licenses makes the product affordable to small businesses. The Microsoft product is targeted for businesses with fewer than 75 users, and includes their Windows 2003 Server. It is priced under $1499 for 5 users, with additional user access licenses at $99 each, or $3500 for 25 users. A 75-user system would cost the business less than $8,500. The Novell product is targeted for businesses

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

with 100 users or less, and includes their Novell Netware Server 6.5, Groupwise 6.5, ZENworks for Desktop, and Border manager. This is priced under $1700 for 25-users, and is actually free with a five user license. A 75-user system would cost less than $4,700.

From a technical perspective, Microsoft offers:

- A secure file and print server with an LDAP compatible directory service (Active Directory).
- A web server (IIS 6.0) that supports the .Net framework, ADO.NET, ASP.NET, XML, IISAPI, Frontpage server extensions and WEBDAV.
- A multi-layered firewall (ISA server) that supports stateful inspection, and packet level, circuit level and application level screening. It also supports Network Address Translation (NAT), access control, Virtual Private Network (VPN), and a high performance web cache.
- A Groupware/email/calendaring package (Exchange server) that includes WebAccess, SMTP, POP3, IMAP, NNTP, and is LDAP integrated. An instant messenger application is also part of this package.
- DNS, DHCP, Certificate and FTP services.
- Terminal services, allowing remote desktop protocol connection sessions to the server for multiple users.
- Team collaboration using the Windows Sharepoint application.
- A full featured database server (SQL Server 2000) that can be integrated with web applications.
- A web page development package (Frontpage 2003).

The Novell package includes:

- A secure file and print server with an LDAP compatible directory service (e-Directory) that supports Novell file sharing protocols, Windows SMB protocols, Unix NFS protocols and Macintosh protocols.
- A Web server that supports Apache 2.0, MySQL, PERL, PHP, Tomcat and allows running and modifying J2EE applications.
- A full featured stateful inspection firewall that supports Packet filtering, Proxy Services, Access Control, SOCKS Gateway, Network Address Translation (NAT), Virtual Private Network (VPN), forward and reverse Web Caching, Alerting and authentication services, including RADIUS support.
- A Groupware/email/calendaring/Document management package that includes Web access, SMTP, POP3, IMAP, and is LDAP integrated. An Instant Messenger application is also part of this package.
- DNS, DHCP, Certificate and FTP services.
- A remote management application (ZENworks) that allows for automated distribution of applications, patches and virus updates to desktops, desktop lockdown, remote desktop management, automated hardware and software inventory from desktops for auditing.

It takes a very technically capable person to be able to install these operating systems, with all of these products on a single server. Different technical expertise is required to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

set up the NAT, Firewall and VPN to function correctly, while still giving sufficient security on that single server. Adding requirements for connecting inbound to the email WebAccess, or to the Web server component, requires additional configuration rules not installed by default in the firewall.

This report will address measures that can be taken to make these types of products more secure. It is not within the scope of this document to address each issue having to do with the individual components of these complex applications. Furthermore, the nature, strengths, and weaknesses of the Microsoft operating system are fairly well explored, and are under constant scrutiny. So, the primary focus of this document will be an overview of the Novell Netware Small Business suite, its higher-level security issues, and a few specifics about individual applications.

Novell Netware and TCP/IP

Starting with Netware 5.0, Novell has moved from IPX protocol layer products to the TCP/IP stack. The broader market had begun to call for open protocols and standardization, and the growth of the Internet was causing a large increase in the capability, desire and need for businesses to connect together. Another general trend was for router manufacturers to not support IPX broadly, limiting IPX routing to a niche market.

Prior to Netware 5.0, operating system software was written around IPX functions and routines, and converted IPX to IP for network consumption. [CTA]. An inherent reduction in performance was the result of this dual-direction IPX to IP translation. In Netware 5 the biggest change was the addition of true support for TCP/IP. [GASKIN1].

In Netware 6.0 the operating system communicates with IP functions and routines natively, resulting in an increase in performance from the previous version. It is completely independent of the IPX protocol, and operates around TCP/IP following the standards and RFC's that TCP/IP is based on. It is as interoperable with other TCP/IP operating systems as any other operating system is, such as Microsoft Windows. No traces of IPX/SPX are left on the network after you choose IP as the default protocol. [GASKIN3].

Netware has had a reputation for strong security, for several reasons. One is that Novell used the IPX and SPX protocols rather than TCP or UDP, and most hackers were not familiar enough with those protocols to spend the time hacking against them. As with most other operating systems, few of Netware's security features are enabled by default. [FOUST1] It is necessary to configure some of these security features in order to make a server safe in today's environment.

With the change to IP only in Novell, the operating system is subject to the same attacks that other IP operating systems have faced, including attacks against well-known ports and protocols, and denial of service attacks.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A Novell Small Business Suite install can, out of the box, install a number of applications and services, all operating on one physical server. This one server then operates as a file and print server, and a firewall providing NAT with multiple Network Interface Cards (NICs); it holds the master partition for the directory service, and acts as the certificate server, email server, LDAP server, DNS, DHCP, FTP, Web server, VPN server and the Backup server. Since Novell uses the TCP/IP protocol, all of these services are available on the local area network, or the wide area network, depending on the configuration of the server.

The list is more extensive with Netware 6.5.

Below are applications on a NetWare 6 server and the default ports that they might have in use. The notation of "no", "yes" and "dependant" represent the ability to adjust the port. The notation of "un" represents unknown.

AFP "548 no"
Apache "80 yes,443 yes"
Border Manager "21 no,119 no,443 yes,1040 no,1045 no, 1959 no,7070 no,8080 no,9090 no"
CIFS "139 unknown"
CsAudit "2000 yes"
DirXML NDS-to-NDS "8090 yes"
DirXML Remote Loader "8000 yes"
DNS "53 no"
eGuide "389 dependant, 636 dependant"
FTP "20 no,21no"
GW Monitor "1099 yes"
GW MTA "3800 (http-6x) yes,7100 (MTP) yes,7180 (http-55EP) yes"
GW POA "1677 (CS) yes,2800 (http-6x) yes,7101 (MTP) yes,7181 (http-55EP) yes"
GW Web Access "80 (http) dependant, 443 (https) dependant, 7205 (agent) yes"
GWIA "25 (smtp) no,110 (POP3) no,(IMAP4) 143 no,389 (LDAP) no, 636 (LDAP-SSL) no, 9850 (http monitor) yes"
iChain "2222 yes"
iFolder "80 (http) dependant,389 (ldap) dependant, 443 (https) dependant, 636 (LDAP-SSL) dependant"
iMonitor "80 (http) yes"
iPrint "443 no, 631 no"
LDAP "389 yes, 636 yes"
Licensing (NLSRUP) "21571 un,21572 un"
LPR "515 un"
Media Server "554 no"
NAS NetDevice "2222 no"
NCP "524 no"
NDPS Manager "3396 no"
NDPS Broker "3014 no"
NDPS SRS "3018 no"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

NDPS ENS "3016 no"
NDPS RMS "3019 no"
NDPS ENS Listener "3017 no"
NetWare GUI "9000 yes, 9001 yes"
NetWare Web Access "80 dependant"
News Server "119 yes"
NFS "20 no,111 no,2049 yes"
NIMS "25,80,81,110,143,389,443,444,465,636,689,993,995 all un"
NMAS "1242 un"
7Novonyx Web Server "80 yes, 443 yes"
NRM "80 un, 81 un,8008 yes, 8009 yes"
NTP "123 no"
NWIP "396 no"
Portal Services "80 dependant,443 dependant,8080 dependant"
Radius "1812 yes"
Remote Console DOS "2034 yes"
Remote Console Java "2034 yes,2036 yes, 2037 yes"
SCMD "2302 no"
SLP "427 no"
SNMP "161 un"
Telnet "23 no"
Tomcat "8080 yes"
VPN "213 no,353 no,2010 yes"
Web Manager "2200 yes"
WebSphere "8110 un"
ZFD 3 "2544 yes,2638 yes, 5008 un,8039 no"
ZFS 2 "80,443,8008,8009 all dependant,1229 no, 1521 yes, 1600 un,2544 yes,2638 yes, 5008 un"
ZFS 3.2 "80,443 dependant, 1229 yes,1433 yes,1521 yes,2638 yes,8089 yes, 65443 yes"

The list is more extensive with Netware 6.5. [NOVELLTID10065719].

A temporary situation exists where many people, including much of the existing Novell customer base and Novell certified engineers, still have the opinion that the Netware operating system is extremely secure, and other operating systems are not as secure. However, because of the move to become completely TCP/IP based, Netware may, arguably, be even *less* secure than other operating systems.

Clearly all of the conventional wisdom relating to securing a network operating system needs to be applied to Novell's Small Business Server. But because of its unique nature, other measures should be considered as well.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Recommendations to make Novell SBS more secure

Like other operating systems, the first step is to install the Small Business Suite with as few applications or services as is needed. In this case,

- Is the FTP server necessary?
- Do the Windows, Unix and Macintosh protocols really need to be supported on your small network? They should not be installed (Native File Access Protocols - NFAP) or they should be disabled unless absolutely necessary.
- Great features of Novell not often advertised are the iFolder, Netstorage and iPrint services. As useful as they are, do they really need to be used?

For all three of these questions, the answer is "probably not" for most small businesses.

The author believes that it is foolish to install the Border Manager firewall and all of the other services on the same Server. Two other options include:

- Install Border Manager on a separate computer, by itself. The Border Manager option is good if the full features that this firewall provides are needed. A duplicate copy of the directory can be stored on the BM server if there is a problem with the file server.
- Purchase a separate firewall appliance device. In a small business environment, a firewall appliance is usually more than sufficient to meet the needs. Products from Sonic Wall, Watchguard, and Lucent are quite adequate.

Some people consider installing the SBS suite without any firewall at all, in order to save money and reduce complexity. In any small business environment, regardless of the server operating system, it is *essential* that a firewall be in place. In the case of Novell SBS, there are numerous TCP and UDP ports that are available, open, and in use. Although these may not have been taken advantage of (in well known ways) by intruders yet, that may not be true in the future. The lack of a firewall opens these businesses up to potential denial-of-service attacks and other hazards.

When you install the OS for the first time, don't let it allocate the entire SYS volume with all of the disk space. With this version of Novell, NSS works very well. Setting aside, say, 8GB for the SYS volume, and then creating another volume (e.g. "DATA") for users' applications and files leaves a portion of the hard drive unallocated. Then there is extra space available later on for a volume that runs out of space. From a security perspective, keeping users and their data off of the SYS volume reduces security risks.

The Apache web server supplied with Novell is very powerful, and full featured. If a business relies on having the flexibility of customizing web applications, then it works well. However, having the web server hosted by another company is usually a much better, more cost-effective choice. It can also reduce security issues, as the publicly known web site would be on someone else's server, someplace else, instead of on the business' primary server. Because of the nature of Netware 6.5, much of the management and administration is done using the iManager web interface, and various other web based components. They will probably eventually replace the Java based Console1 and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Nwadmin utilities as the basis for administrating Netware. What this means is that a Netware server, even if protected by a firewall, needs to run web based services, and this usually can't and shouldn't be shutdown.

If a separate firewall appliance device is not the option, then putting the DNS and DHCP server (where NAT and VPN are handled) and Certificate server software on the Border Manager makes sense.

Novell's e-Directory is a very stable and secure Directory. It is also LDAP integrated, and as such, vulnerable to LDAP based attacks. Correct configuration of security for e-Directory and LDAP is very important.

The Groupwise application uses the SMTP protocol to communicate to other email servers. In this version, it is not susceptible to being used as an open relay out of the box. POP3 and IMAP should be disabled unless you plan on letting your users connect in to check their email. In a small business environment, establishing Web Access as the method for getting email externally and disabling POP3 and IMAP is recommended. In addition, Groupwise stores all configuration and user information in the directory, and communicates with it using LDAP. The Groupwise Internet Access Agent (GWIA) can be set up to use the SMTP "STARTTLS" command described in RFC2487. SSL can be used to secure POP, IMAP and SMTP. When requiring SSL/TLS connections for SMTP, one must make sure that the Server at the other end will support it also. [KRATZNER2]

The current widespread problem with unauthorized advertising email, also called SPAM, can affect a small business dramatically. Nothing in the Novell SBS directly addresses this issue. One solution is to purchase and install additional software for monitoring and eliminating some SPAM. Products for Novell SBS that can do this include Guinevere, http://www.beginfinite.com/html/guinevere.html
and Gee-Whiz
http://www.omni-ts.com/index.asp?page=products&prod_id=18.

A Gateway solution would also add to the cost, but requires less administrative effort on the part of the small business, and also can help to eliminate other types of security issues. You configure Groupwise to send all outbound email to a host company to be scanned before being sent, and all inbound email can be directed to first go through this same Gateway host. This works by pointing your DNS MX record to their server address.

Two Gateway products, *Ciphertrust*
http://www.ciphertrust.com/solutions/messaging_solutions/groupwise/
and *Message Labs*
(http://www.messagelabs.com/services/portfolio/),
can do anti-virus, anti-Spam, anti-porn and content filtering for inbound and outbound email. They are easy to set-up, administrate, and are inexpensive enough for a small business to afford.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ZENworks
ZENworks is a powerful tool. But, if your small business does not have someone to administrate it, or if you only have two or three desktops, then you should consider not installing and using ZENworks. For a business with a larger number of users, especially if they are at multiple locations, ZENworks can help reduce desktop support issues and help desk calls. The capability to lock down desktops and to self-heal/reload applications can reduce normal day-to-day problems and support expenditures for a small business.

LDAP Security configuration
"LDAP is configured and ready to run with the default settings as soon as it is installed. By default, all users can connect anonymously and query the directory using the [Public] object. They can see any object to which the [Public] object has access. To tighten security, you can create an LDAP proxy user to be the only one with permissions to the objects, containers, and properties that you want people to view using LDAP." [GASKIN3].

This anonymous bind operation is convenient if your LDAP server doesn't contain information that needs to be protected, and you don't want to deal with authentication issues. The administrator can specify exactly which rights an anonymous user has by either setting access controls for the [public] entry, or by setting up a proxy user that is used whenever someone requests an anonymous bind. [HARRISON]. By using the proxy user and setting up the LDAP server to only use SSL communications, you substantially reduce the chance that an unauthorized access to LDAP or eDirectory will occur. Without SSL, LDAP passes the connection password in clear text over the network.

Novell Certificate server is a requirement for providing SSL, and must be installed on your server. This will be installed as the default out of the box, but you must be careful to not remove it from the list of default-installed services when removing other unnecessary services. With Certificate server installed, your server will act as the Organizational Certificate Authority (CA) for your small business. As mentioned earlier, this should be placed wherever the Border Manager application is placed.

Within ConsoleOne, you must modify the LDAP server object to require use of SSL for LDAP, and to configure the SSL certificate. Without doing this, LDAP, and consequently, e-Directory are vulnerable to clear text passwords being passed on your local area network.

Groupwise Security
When setting up Groupwise, you can set up LDAP authentication, so that users do not require a separate password for Groupwise. The eDirectory password will be used instead. There are pros and cons to this. Some people prefer separate passwords for Groupwise users, and some prefer the same passwords. Generally speaking, for a small business, keeping the same password simplifies things, reducing the occurrence of users writing passwords down.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

When doing this it is recommended to set up LDAP to use SSL so that all LDAP communications are encrypted. SSL configuration should be set up when configuring the POA, the MTA, WebAccess and GWIA. By doing this, the individual elements communicate to each other using encrypted communication.

Secure the web server with SSL
Setting up SSL is important to protect your Web server. This can be complex, and is outside the scope of this article. A good reference would be an article in Novell's Netware Connection magazine:
http://www.novell.com/connectionmagazine/2002/10/secure.pdf

Plain old network security recommendations

Novell's reputation for security has always been very high. The first focus of security for Novell has always been physical security. Keeping your server(s) in a physically secured, controlled access location is still the first step in network security.

"Every security policy should start with protecting the server hardware from unauthorized access. That means physically locking away your servers in a secure room. No server is safe when a hacker has direct access to its console. If someone has access to a server, they have free reign to load NLMs from a diskette, switch the server into debug mode, remove NDS from the server, shut down the server, or even remove the server's hard drives". [FOUST1].

Admin Account
After you install Novell, give the "admin" user a password. Rename the "admin" user to something else, but keep it simple. (e.g. "nwadmin".)

Strong Passwords
The two primary methods for password attack are dictionary lookup and brute force attack. Other methods rely on social engineering or someone watching as you type.

There are many recommendations among security professionals as to what constitutes a "strong" password, and to what "length" someone should go to have a strong password. Microsoft's recommendations look like this:

"Make sure you create a password that:
- Is at least seven characters in length, and the longer the better. (Passwords for Microsoft Windows® 2000 and Windows XP can be up to 128 characters long.)
- Includes upper and lower case letters, numerals, symbols
- Has at least one symbol character in the second through sixth position
- Has at least four different characters in your password (no repeats)
- Looks like a sequence of random letters and numbers"

"Make sure you:
- Don't use ANY PART of your logon name for your password
- Don't use any actual word or name in ANY language
- Don't use numbers in place of similar letters

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Don't reuse any portion of your old password
- Don't use consecutive letters or numbers like "abcdefg" or "234567"
- Don't use adjacent keys on your keyboard like "qwerty" "

[MICROSOFT2].
http://www.microsoft.com/security/articles/password.asp

Following the "keep it simple" approach can keep it from being so confusing. You can get 90% of the value for 10% of the work by following just a few of these recommendations.

- Use a phrase rather than a word.
- Make sure the phrase is long (10-20 characters or more).
- Set Intruder Detection parameters to trip on Incorrect Login Attempts = 4, and set the "Lockout After Detection" Interval for an hour. Four bad attempts, and the account is locked out for an hour.

If you set the password policies so that passwords are long, you are taking the *primary* measure. Obscure, hard to remember passwords with upper and lower case or special characters should be *avoided*. The user will only forget them, or write them down. Pass phrases are much more effective. Any phrase over ten characters would be ideal (e.g. "don't tread on me", "oh say can you see", or "my littlered corvette"). The phrase could be with or without spaces, just so it is long. Either of the examples given here would survive a dictionary lookup or brute force attack very well. Limit the number of bad login attempts to three or four, and with a long pass-phrase the chance of it being broken are very, very small. Adding some numbers of significance could make it harder to guess from someone glancing over your shoulder (e.g. "my littlered 1975 corvette").

Auditing
Novell SBS installs the capability for auditing by default. But few businesses have the time or technical expertise to review their audit logs, so this usually takes up extra CPU usage towards no purpose. If a small business has adequate technical or financial resources, and appropriate security concerns, then having a recurring security review that looks through the logs can be beneficial.

Group Security
Set up several groups based on roles. For instance, "controller", "accounting", "shipping", and "sales" are possible groups. Give rights to the directories that you use based on the groups. Put your users in one group or another. Don't give any individual login rights to objects, files or directories. If a user needs rights, and a group having those rights does not exist, create a new group for that, give the group rights, and put that one user in the group. This makes maintaining security much simpler. When someone changes roles, or a new person takes on another person's roles, maintaining and updating security is straightforward.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Console Security
Of course, controlling physical access to the server is the first step, but additionally, you can put a password protected screen saver on the console to prohibit any unauthorized changes if someone does have physical access. In this version of Novell, loading the "scrsave.nlm" does this. Also, it is important to monitor remote access to the console. Historically, "rconsole.exe" allowed this. Rconsole does not come with this version of Novell Netware, however it can be copied from older versions, especially if SBS is an upgrade from a previous version of Novell. Another utility, "rconag6" gives remote control access to your server using TCP/IP. If you use it for the first time with the "Rconag6 encrypt" option, then it will accept and encrypt your password and creates a load file, "ldrconag.ncf" to use to load rconag6 on your server in the future, without needing or displaying the password.

Malicious Code/Virus/Worms
Because of the nature of the threat in today's world when connected to the Internet, having a scanner for malicious code is necessary. Even for the smallest business it should be a requirement. A multi-tiered approach is best, with scanning done on the file server, as well as on the individual desktops. There are numerous potential solutions for managing this aspect of your business. The top commercial vendors are Computer Associates e-trust Antivirus; Symantec Norton Antivirus, NAI McAfee and Trend Micro, all of whom have a Novell Server version of their product, and desktop versions of their products.
http://www.my-etrust.com/
http://www.symantec.com/product/
http://us.mcafee.com/default.asp
http://www.trendmicro.com/en/home/us/personal.htm

There are also numerous FREE antiviral packages including:

Grisoft AVG Antivirus (for sale and free version. Not available for Novell Server).
http://www.grisoft.com/us/us_avg_index.php

http://www.f-prot.com/download/ (For sale and free version for home use, commercial use must be paid. Not available for Novell Server)

Eset NOD 32
http://www.nod32.com/download/trial.htm (Free for home use, commercial use must be paid. CACPAC].

The DAT file that contains the updated list of malicious code should be updated from the provider on at least a daily basis. A previous scheme of updating once a month, or once a week is not sufficient.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Backups
Current backup devices often used include DLT or AIT tape drives. DAT drives are older technology, and should be avoided unless the budget is so small that no other options are available. One of your servers (or your only server) will have this attached. With a small business, and hopefully not too much data, setting up tape backup software to backup ALL data every night may be possible, and is more desirable than incremental, or differential backups. Don't forget to get a backup of NDS/eDirectory also. If full backups to one tape are possible, then setting aside a series of tapes, and following a schedule should be done. My recommendation would be to have a Monday, Tuesday, Wednesday and Thursday tape, and then five Friday tapes, labeled Friday1 through Friday5. You can hand write on a calendar which Friday tape is for each Friday in the month. Some businesses may require, or desire more backups that this and you could extend this scheme from five tapes to 13 tapes, 26 tapes, or whatever. Some businesses pull one or more of their Friday tapes from time to time and put them off-site, replacing them with a new tape.

The key issues with backups are pretty similar to those with larger businesses.

- Keep backup tapes off-site, in case some disaster happens to your site.
- Keep the tapes secure, whether they are on-site or off-site. If an attacker gets your tapes -- they get your business data.
- Too many businesses change tapes regularly without testing their backup, only to find later that they have no backup, or that the good backup does not have the data they needed. Testing the backup by restoring data should be done regularly.

Data shows that 73 percent of businesses that suffer a disaster are out of business within three years. And 43 percent don't even survive the first year.
[NUCIFORA]. With the range of small businesses that we are discussing here, the statistics would probably be more dramatic.

For a small business, cash flow is extremely important. Losing accounting data to a disaster (such as a fire, or a bad hard drive, or users inadvertently deleting files, etc.) could shut the business down.

Security Audits
Having a security expert review the final installed configuration after the network engineer installs the operating system and components is important. Because of the broad nature of installing the operating system, a network engineer may not have the specialized expertise with the more detailed security issues. In most installs often the components are left as installed right out of the box.

Having recurring security audits of your system on perhaps an annual basis can be valuable. Because of limited budgets, sizing the audit to cover the important issues while minimizing costs is necessary.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Acceptable-Use Policy

In a small company, acceptable use of the business' computers and Internet access may seem to be common sense. Many companies have a set of "unwritten" rules that they expect their employees to go by. This may work with a two or three person office. It's not news that as a company grows the potential for liability grows.

The discussion of acceptable use is a long topic in itself. The important aspect of this is the potential liability if your employees mistakenly do the wrong thing. The most apparent types of inappropriate use that can create difficulties include loss of productivity, and liability for offensive content.

"As an example, federal law now requires companies in the United States with 25 or more employees to provide a work environment free of gender, ethnic, and racial harassment or discrimination. That requires taking reasonable steps to eliminate harassing materials from the workplace. Illegal or offensive content may include:

- Pornographic images downloaded off the Web
- Pornographic or racially offensive e-mail attachments
- Offensive language or words

It may not matter whether the company knew employees were downloading pornographic images. The test at trial is whether well-known remedies were available to prevent abuses, whether a policy existed to apply those remedies, and whether the policy was actually enforced." [MERRITT].

Fairly recent legislation has created a series of limitations on how to do business with certain other businesses. These include:

- *Sarbane-Oxley Act (2002), which* affects financial services, accounting, auditing, financial reporting and professional services firms.

- *Gramm-Leach-Bliley Act (1999),* which affects banks, securities firms, and insurance companies

- *Health Insurance Portability and Privacy Act (1996).* Commonly referred to as HIPPA, includes National Standards for Transactions, Security, and Privacy, of certain types of health data.

[MERRITT].

These issues just adds another level of complexity to your business, beyond the technical security issues and are outside the scope of this document. The advice of Security Professionals is essential here.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Summary

The Novell Small Business Suite is a powerful tool for a small business, at a low price. Because small businesses have limited budgets, they have limited capability to install, configure, patch and maintain their servers. Because of the technical complexity of such products, it can be easy for security holes to be found and taken advantage of without a small business being aware. I have barely touched the surface of the issues that could be discussed with each of these features and services. Potentially, each of these could be the topic of a paper (Border Manager rules, Groupwise Email configuration, Security Auditing, Malicious code prevention, Web Security, Etc.) Having the operating system and various components installed and configured by an expert is very important, as the “out of the box” install leaves numerous vulnerabilities that could potentially be a realized threat to your business. Having recurring security audits sized for your small business environment is also important to reducing and minimizing these vulnerabilities.

© SANS Institute 2003, Author retains full rights.

References

[ABEND1]
Dear ab-end, Configuring LDAP to Use SSL, Novell AppNotes, Volume 14, Number 05, May 2003. URL:
http://developer.novell.com/research/sections/netsupport/abend/2003/may/x030501.htm

[ABEND2]
Dear ab-end, eDirectory Account Creation Via LDAP, Novell AppNotes, Volume 13, Number 12, December 2002. URL:
http://developer.novell.com/research/sections/netsupport/abend/2002/december/x021201.htm

[ABEND3]
Dear ab-end, Used IP Ports in NetWare 6. Novell AppNotes, Volume 13, Number 04, April 2002. URL:
http://developer.novell.com/research/sections/netsupport/abend/2002/april/x020401.htm

[BALASUBRAMANIAM]
Balasubramaniam, M; Ganapathi, CH; Rajan, BT; IP Address Management Framework: Managing Application IP Address/Port Configurations in NetWare 6.5. Novell AppNotes, Volume 14, Number 09, September, 2003.
URL: http://developer.novell.com/research/appnotes/2003/septembe/02/a030902.htm

[CACPAC]
Penn State University, Virus Detection/Removal Software for the PC, CAC Internet Software Distribution
URL: http://ftp.aset.psu.edu/pub/ger/documents/virus.htm (6 June 2003).

[CENSUS]
U.S. Census Bureau, United States Department of Commerce, Statistics of U.S. Business Table 2a
URL: http://www.census.gov/epcd/www/smallbus.html

[CTA]
Computer Training Academy, "Netware 5 and TCP/IP Support", July 14th, 1998.
URL: http://www.cta.net/whoweare/whoweare_press.asp?article=11&selYear=1998

[DAY]
Day, Martin, Protecting your Network from Hackers with Advanced BorderManager Packet Filtering. Novell AppNotes, Volume 11, Number 09, August 24th, 2000.
URL: http://developer.novell.com/research/appnotes/2000/septembe/02/a000902.htm
URL: http://developer.novell.com/research/appnotes/2000/septembe/02/a0009025.htm

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[FONTANA]
Fontana, John; Spam filters revealing their darker side. Network World, September, 9th, 2002.
URL: http://www.nwfusion.com/news/2002/0909spam.html

[FOUST1]
Foust, Mark, Netware Security: Closing the Door to Hackers. Novell AppNotes, Volume 11, Number 06, June 7th, 2000.
URL: http://developer.novell.com/research/appnotes/2000/june/03/a0006034.htm

[FOUST2]
Foust, Mark, NetWare's Security Track Record
Novell AppNotes, Volume 11, Number 06, June 7th, 2000
http://developer.novell.com/research/appnotes/2000/june/03/a0006032.htm

[FOUST3]
Foust, Mark, Auditing NetWare Security
Novell AppNotes, Volume 11, Number 06, June 7th, 2000
URL: http://developer.novell.com/research/appnotes/2000/june/03/a0006011.htm

[GASKIN1]
Gaskin, James E., A Short History of Netware. 2000.
URL: http://www.masteringnetware.com/History/history.htm

[GASKIN2]
Gaskin, James E., Mastering Netware 5.1. Alameda, CA: Sybex, Inc., 2000.

[GASKIN3]
Gaskin, James E., Mastering Netware 6. Alameda, CA.: Sybex, Inc., 2002.

[GROSS]
Gross, Grant; Small business owners disagree on Spam approach. Network World Fusion, October 30th, 2002.
URL: http://www.nwfusion.com/news/2002/0909spam.html

[HARRISON]
Harrison, Roger E., Sermersheim, Jim and Trottier, Steve, Novell's LDAP Developer's Guide, Novell Press, IDG Books Worldwide, 2000.

[HSBC]
House Small Business Committee. U.S. House of Representatives,
URL: http://www.house.gov/smbiz/facts/

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[KRATZNER1]
Kratzner, Tay, Securing a Web Server on Netware. Netware Connection, October 2002, 26-29.
URL: http://www.novell.com/connectionmagazine/2002/10/secure.pdf

[KRATZNER2]
Kratzner, Tay, Novell's Groupwise 6 Administrator's Guide. Novell Press, New York: Hungry Minds, Inc., 2002.

[LYON]
Lyon, Rob; Installing and Configuring NetWare AMP (NetWare 6, Apache, MySQL, and PHP/Perl), Novell AppNotes, Volume 13, Number 12, December 2002. URL: http://developer.novell.com/research/appnotes/2002/december/05/a021205.htm

[MATILLA]
Matilla, Darren, Securing Novell Netware 6, GIAC Security Essentials Certifications Practical Assignment, September 4, 2002.
URL: http://www.sans.org/rr/papers/index.php?id=908

[MATHUR]
Mathur, Raj, Administering and Securing Apache 2.0, Skillsoft Press, 2003.

[MCKELL]
McKell, Mark, Taking Advantage of NetWare's Public Key Infrastructure with Novell Certificate Server 2.0 Novell AppNotes, Volume 11, Number 01, August 24th, 2000
URL: http://developer.novell.com/research/appnotes/2000/january/05/index.htm

[MERRITT]
Merritt, Tony, Creating and Enforcing an Internet Acceptable Use Policy. Novell AppNotes, Volume 14, Number 04, April 2003.
URL: http://developer.novell.com/research/appnotes/2003/april/02/a030402.htm

[MICROSOFT]
Microsoft Windows Small Business Server 2003, Product Page
URL: http://www.microsoft.com/windowsserver2003/sbs/default.mspx

[MICROSOFT2]
Microsoft, Checklist: Create Strong Passwords
URL: http://www.microsoft.com/security/articles/password.asp

[NAY]
Nay, Krt; Cadjan, Nancy; Taking Things Out of Context: Using LDAP Contextless Login in Your Network, Novell AppNotes, Volume 14, Number 09, September, 2003.
URL: http://developer.novell.com/research/appnotes/2003/septembe/01/a030901.htm

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[NEFF]
Neff, Ken; What's New in NetWare 6.5? Novell AppNotes, Volume 14, Number 08, August, 2003.
URL: http://developer.novell.com/research/appnotes/2003/august/01/a030801.htm

[NORTHCRAFT]
Northcraft, Justin, Assessing and Securing a Novell Netware Environment, GIAC Security Essentials Certifications Practical Assignment, January 19, 2003
URL: http://www.sans.org/rr/papers/index.php?id=908

[NOVAK1]
Novak, Kevin, Securing Your Netware Environment, Network Computing, October 16th, 2000, Kevin Novak (knovak@neohapsis.com)
URL: http://www.networkcomputing.com/1120/1120ws1.html
URL: http://secinf.net/netware/Securing_Your_NetWare_Environment_.html

[NOVAK2]
Novak, Kevin, Authentication at its finest, Network Computing, October 16th, 2000
URL: http://www.networkcomputing.com/1120/1120ws1side1.html

[NOVELL1]
Novell Small Business Suite, Product Page
URL: http://www.novell.com/products/smallbiz

[NOVELL2] Netware 6.5, Novell Documentation
URL: http://www.novell.com/documentation/lg/nw65/index.html

[NOVELL3]
Overview of Novell Web and Application Services in NetWare 6.5 Novell AppNotes, Volume 14, Number 08, August, 2003.
URL: http://developer.novell.com/research/appnotes/2003/august/05/a030805.htm

[NOVELLTID10065719]
Matrix of Ports used in NW6, Technical Information Document 10065719,
URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10065719.htm

[NUCIFORA]
Nucifora, Alf, Mitigate Business Disaster with a Business Plan, Orlando Business Journal, November 5, 2001.
URL: http://www.bizjournals.com/orlando/stories/2001/11/05/smallb1.html?jst=s_rs_hl

[RICHICI]
Richichi, Mike; How to Use Perl, Python, and PHP to Access eDirectory 8.7 via LDAP. Novell AppNotes, Volume 14, Number 05, May 2003.
URL: http://developer.novell.com/research/appnotes/2003/may/04/a030504.htm

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[RILEY]
Riley, Cyndi, What You Get in Novell's Small Business Suite 6. Novell AppNotes, Volume 13, Number 09, September 2002. URL: http://developer.novell.com/research/sections/netmanage/smallbiz/2002/septembe/s020901.htm

[SANDERSON]
Sanderson, Mark, Netware 4 and 5 Security Guide and Checklist, GIAC Security Essentials Certifications Practical Assignment, September 5th, 2001.
URL: http://www.sans.org/rr/papers/index.php?id=9248

[THOMPSON]
Thompson, Paul, Tips for Running iFolder and BorderManager Together. Tips and Tricks, Novell AppNotes, Volume 13, Number 10, October 2002. URL: http://developer.novell.com/research/sections/netmanage/tips/2002/october/t021001.htm

[UFOIT]
Best Practices for Netware Security. Office of Information Technology, University of Florida, October 21st, 1999.
URL: http://grove.ufl.edu/~pbc/itsa/netware-security.html

[USSBA]
U.S. Small Business Administration, Small Business by the Numbers: 2001.
URL: http://www.sba.gov/advo/stats/sbfaq.pdf

[WILLIAMSON]
Williamson, Marcus, Implementing Strong Passwords in an NDS Environment. . Novell AppNotes, Volume 11, Number 08, August 2000. URL: http://developer.novell.com/research/appnotes/2000/august/02/a000802.htm

© SANS Institute 2003, Author retains full rights

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced