



Handling the Three Major Types of Threats

Network Security in a New World

The events of this past fall have brought about a new interest in computer network security. We define Computer Network Security as the two part goal of minimizing unplanned service outages and guaranteeing data safety and integrity. At Dominant Systems, we stand ready to assist our customers in reaching this goal.

Achieving Network Security involves understanding and preparing for three distinct types of threats, each with their own unique characteristics. These threats are: 1) External Threats, such as those coming in from the internet; 2) Internal Threats, such as those from disgruntled employees and corporate spies; and 3) Threats from hardware and software failures. Each can result in network service outages plus lost, stolen, or corrupted data.

EXTERNAL THREATS

Networks that are connected to the internet are the most vulnerable to external threats. Two basic

types of external threats exist, viruses and hacker attacks (unauthorized intrusions).

Viruses

For virus protection we recommend a server-based virus protection program like Norton Anti-virus Corporate Edition. Once installed on the server, products of this type will automatically download the latest virus signature files, and "push" them out to each workstation. Many email packages can also be set up to limit the types of attachments that are allowed to be included with an email. Since most viruses infect systems when an unsuspecting user opens an email attachment, disallowing most types of attachments can prevent many viruses from spreading.

Hacker Attacks

Security attacks from unauthorized users (hackers) is a growing problem for today's network administrators. The authors of the best-selling

(continued on page 2)

Take Control of your Network Security with DSC Network Security Services

Whether you need network design or simply to improve security on your Internet connection, Dominant Systems Corporation has a team of experts who can smoothly integrate your corporate security policies into your computer network. Our staff of consultants and engineers has 15 years of proven expertise in designing, implementing, and supporting computer network security solutions. By conducting a security assessment, we can quickly identify potential risk from hacker intrusion, virus attack, or network downtime due to hardware or software failures. Our assessment progresses in four stages. Each stage provides feedback to you regarding the state of your network.

1. Phone Consultation

Dominant Systems recognizes that integrating dozens of products into a secure network infrastructure requires true network architects who have proven expertise in designing security solutions. The process begins with a phone call to one of our experts. Please call 734-971-1210 for more information.

2. Snapshot Internet Security Scan

The Internet is a publicly accessible network and can represent a security risk to any business. Using the same tools that hackers use, one of our experienced engineers will scan your Internet connection and assess any vulnerability.

(continued on page 3)

TECH TIPS

Use Passwords That Are Difficult To Crack.

A good corporate password policy should include these rules at the minimum.

- 1) Do not use real words as passwords. Most password cracking programs contain large lists of words and word endings.
- 2) Use non-alphanumeric characters like "!" and "&" sprinkled throughout the password
- 3) Set passwords to expire after a period of time no longer than 6 months.
- 4) Make sure all accounts on your server are required to use a password (no "blank" passwords). Such passwords should be at least 7 characters long.

5) Because of a quirk in the way Windows NT and 2000 store their passwords, it is best to use 7 character or 14 character passwords. In any case, passwords should never be less than seven characters long.

Strong PWs	Weak PWs
hip0chondr1ac!	Spot
!F0rty440years	mypassword
sch!z0phren!c2	daisy

Update Virus Software

Install the corporate edition of a good antivirus program (like Norton AntiVirus) on all servers and workstations. You can then set up your server to "push" updates to the workstations as they become available.

Network Security In A New World

(continued from page 1)

book "Hacking Exposed : Network Security Secrets & Solutions" have this to say about the problem. "As experienced security practitioners who are immersed in the field each day, we can confidently say that the problem is much worse than everything you've heard or read".

For dealing with external threats, we recommend using the CERT (Computer Emergency Response Team) approach which is documented in the book *The CERT Guide to System and Network Security Practices*. This program is broken up into five sections: Harden & Secure; Prepare; Detect; Respond; and Improve.

1. Harden & Secure

- a. Install firewall and anti-virus software on all systems, especially those with access to the outside world.
- b. Apply all patches and updates for your system and application software.
- c. Disable all server software services that are not necessary for operation.
- d. Remove all network user permissions following the principle of "deny first, then allow". Begin by removing all access privileges to everyone, and then selectively grant access as needed.
- e. Enable event logging functions on all devices so that in case of a problem, detailed information will be available to help figure out what happened.

2. Prepare

Since not all security holes are known at any given time, it pays to prepare for those risks as well.

- a. Identify additional security concerns not covered in Step 1.
- b. Develop policies, procedures and systems to minimize those concerns.
- c. Install intrusion-detection systems.

3. Detect

Analyze logs, system events and user problems to detect potential security breaches.

4. Respond

- a. Analyze the effects of, scope of, and damage caused by the intrusion.
- b. Recover from the attack by getting systems back to normal operations.

5. Improve

This step usually occurs after a new intrusion or threat has been identified.

- a. Hold a post-mortem to discuss what was learned.
- b. Update policies and procedures.
- c. Re-examine steps one through three, and make any necessary changes.

INTERNAL THREATS

Internal threats are those that typically come from inside the organization. Disgruntled and/or curious employees, corporate spies and employee error are the main types of internal threats. Dealing with internal threats is a three step process.

1. Physical Security

- a. Keep your servers and connectivity equipment in a locked room.
- b. Make sure environmental conditions in your server room are within the guidelines for the equipment used.

2. File Security

- a. Verify that users only have access to files, directories and programs that they need to perform their work.
- b. Verify that inactive accounts have been terminated.

3. Acceptable use policies (AUP's)

Every company needs an AUP for their network, but because each organization is different, there is no all-purpose policy that every company can use. Some rules to consider for your AUP include:

- a. Only systems administrators are allowed to install software on the network.
- b. No game software is to be installed.
- c. No public domain software is to be installed, unless it is first tested off the network.
- d. Use "Strong" passwords only (see Tech Tips on page 1), and force users to change passwords at least every six months.

HARDWARE FAILURES

Hardware and software failures are easily the most common problems that affect Network Security. When critical components fail, unplanned service outages are often the result. These outages are the easiest to prevent, however, and can be minimized by proper planning and the use of redundant components in your servers. Servers with

mirrored disks or RAID disk subsystems have the ability to keep on running even if one of the disk drives fail. Redundant disk controllers can make a disk subsystem even more bullet-proof.

Power supplies are another component that has a high likelihood of failure. Many new server models such as Compaq's Proliant ML370 have optional redundant power supplies that consist of 4 separate power supplies controlled by a circuit board. When one of the units fails, the board detects it, and automatically adjust its power consumption to the other three. For systems that do not offer redundant features, consider keeping spare components on hand.

Installing a good tape backup system is also critical to maintaining data safety and hence Network Security. Server class tape backup systems typically use DAT, AIT, or DLT media. Backups should be done once a day using a set of tapes, not just one tape. Rotate one of them into your tape archive at least once a month and replace it with a new tape. Periodically check that the backups you are making are still readable by doing a sample restore from one of your recent tapes.

Installing power backup (UPS) systems on all network components will prevent those components from interrupting network service if there is a temporary power failure.

SUMMARY

Creating a secure network involves being prepared for external and internal security risks as well as hardware and software failures. While no computer network can be 100% immune to unplanned outages or data loss, the above guidelines can help strengthen the security of any network.

For many overworked network administrators, the time required to plan and administer a secure corporate network is simply not available. Fortunately, Dominant Systems has developed a set of packaged security services that can assist companies wishing to improve their network security. Please call us at +1.734.971.1210 for more information.

DSC Packaged Security Services

(continued from page 1)

The engineer will provide a security grade and a comprehensive report. Our focus for this service is on the small to medium size business. This report is designed to be accurate yet affordable. Typically, a scan can be completed within a few hours. It provides a snapshot of your Internet connection vulnerabilities and suggestions for security improvements.

3. Comprehensive Assessment

The majority of security-related issues occur from inside a corporate network. An expensive firewall solution cannot protect you from a disgruntled employee or faulty data backups. Building on the results of our Snapshot Internet Scan Report, one of our security engineers will use industry standard techniques to examine the security of your internal network infrastructure in the following key areas:

Physical Security

Check server room accessibility, electrical, and environmental issues.

File Security

Scan for viruses, trojan horses, and unprotected services. Verify permissions, data backups, and security patches.

User Security

Evaluate password strength, inactive accounts, passwords on sticky notes.

Remote Access

Verify security on PCAnywhere systems, VPNs, and dial-in modems.

Firewall Rule Set

Check file sharing, open ports, and insecure services.

Security Planning

Evaluate network diagram and documentation, password guidelines, and recovery plans.

A comprehensive assessment will take several days to complete. The engineer will provide a written report detailing any security issues as well as our recommendations for improving security on your network.

4. Problem Remediation

Once problems have been uncovered, our security experts are available to fix them.

While no network can be made 100% safe, our packaged security services can add layers of defense to your networks, minimizing the possibility of security related downtime. Call us at +1.734.971.1210 for more info.

The Top Ten Computer Network Vulnerabilities

1. Lack of hardware fault-tolerance and redundancy.
2. Inadequate or unreliable tape backup devices, media, and use policies.
3. Inadequate router access control and/or missing or improperly installed firewalls.
4. Unsecured and unmonitored remote access points like PCAnywhere hosts.
5. User accounts with excessive privileges.
6. Outdated or unpatched software, or software left in a default configuration.
7. Lack of accepted and policed security policies and procedures.
8. Weak and re-used passwords.
9. Misconfigured internet servers
10. Inadequate logging, monitoring, and detection capabilities.

The Dominant View: Nimda Worm, Network Reliability

by Terrence A. Weadock

Organizations in our service area continue to be hit with various network disruptions mostly caused by poor or non-existent security policies and procedures. During the week of September 10-14, 2001 our Help Desk helped over 25 sites that needed assistance battling the Nimda worm. Based on our experience, this was the worst virus to ever hit our customers.

The good news is that most sites were back up and running by the next week. The bad news is that these organizations lost many labor hours of productivity and were saddled with substantial repair bills. While there will always be new security threats on the horizon, a solid plan for dealing with them is essential to limiting the harm they can cause. While we are talking about service disruptions

and network reliability, it is only fair to mention problems that are not caused by outside agents. I have compiled the Dominant Systems Top 5 Reliability Problems to address this.

1. Using non-data-processing quality systems in a commercial environment. These types of equipment include no-name clones, systems made for home use such as Compaq Presario and HP Pavillion systems, and systems purchased because they were the cheapest available. The costs of supporting such systems can easily outweigh the costs of simply replacing them
2. Using non-data-processing quality operating systems. These include Windows 95, Windows 98, and Windows ME. The amount

of lost productivity from using these OSES is truly staggering. Each time one of these crashes, it has the potential to foul up the entire network plus the application software and databases that run on it.

3. Allowing users to install whatever software they want on the network. This is a great way to get destructive computer viruses and simultaneously run afoul of anti-piracy laws.
4. Not having a long-term plan for their networks.
5. Using unreliable tape backup hardware, software, and media rotation schemes.

Terrence A. Weadock is the President and founder of Dominant Systems.



DOMINANT SYSTEMS

4201 Varsity Drive, Suite D, Ann Arbor, MI 48108

+1.734.971.1210

+1.734.677.3321 Fax

<http://www.domsys.com>

Prsrt Std
U.S. Postage
Paid
Permit #78
Milford, MI

Inside this issue of ***THE HIGH PERFORMANCE NETWORK NEWS***

**NETWORK SECURITY IN A NEW WORLD - How to Protect Your Network.
NETWORK SECURITY SERVICES from Dominant Systems.
THE TOP TEN COMPUTER NETWORK VULNERABILITIES.
THE DOMINANT VIEW: Viruses, Network Reliability.**

COUPON

Is your Network vulnerable to External Threats?

Find out with a

Snapshot Internet Security Assessment

Using the same software tools that hackers use, one of our experienced engineers will scan your Internet connection and assess any vulnerability. We will then provide a security grade and a comprehensive report detailing the vulnerabilities we have found.

FREE*

Regular Price
\$599

Computer Networks
Since 1987



DOMINANT SYSTEMS

4201 Varsity Drive, Suite D, Ann Arbor, MI 48108

+1.734.971.1210

+1.734.677.3321 Fax

<http://www.domsys.com>

*Available to qualified businesses and organizations with this coupon that are located in Michigan, Ohio and Indiana only. A signed Client Authorization form must be completed in its entirety to begin work. Offer expires on 1/31/02.

Dominant Systems

Work with the Experts. Enjoy the Security.

Authorized Sales

Compaq
Cisco
Citrix
Hewlett Packard
Legato
Microsoft
Novell
Caldera (SCO)
Symantec
Veritas

Service & Support

Consulting
Project Management
Network Administration
Network Security
Disaster Recovery
On-site Service
Carry-In Service
Help Desk Support
Windows NT, 2000 & XP
Netware & UNIX

Solutions

Local Area Networks
Wide Area Networks
Fault Tolerant Servers
Firewalls
Remote Access
Intrusion Detection
Upgrades
Virus Protection

Call Us Today!
+1.734.971.1210
or visit our Web Site at
www.domsys.com