Practical Aspects of Network Security A Down-to-earth Approach

Jaya Prasad, ME, Comp. Sc., Professor
Department of Computer Science and Engineering
New Horizon College of Engineering, Bangalore, India
ravi8910@gmail.com

Abstract: Practical network security is all about finding the right balance between protecting your business interests and resources, and letting people get their jobs done. This article describes the practical network security assessment, how secure is your system Internet, virus (downloadable from Internet), steps towards securing a network and role of organizational staff. [The Journal of American Science. 2007;3(1):10-12].

Keywords: Internet; network security; virus

1.0 Introducing Practical Network Security:

Practical security is all about finding the right balance between protecting your business interests and resources, and letting people get their jobs done. Everyone is aware of the threats. Establishing a network security strategy is only feasible, however, if you understand that the biggest obstacles you'll grapple with may well come from within your organization. A security plan that addresses your critical business concerns – customer confidence, data integrity, increased productivity, and cost savings – will give you the business advantage by thoroughly targeting security fissures at their source: the people and their processes

1.1 Security Assessment:

Your security development process should be a precise, all-encompassing, methodical approach to creating a long-term security solution. You will need to analyze your assets and the threats to them, and quantify in time, money, and business reputation what these threats may cost your business. Next, identify your system vulnerabilities and calculate your level of risk, and examine and identify elements that are outside of your control (laws, corporate culture, budget, etc.)

The first thing you need to do to develop effective security is to establish a team that will work with you to gather and analyze all of the information. But before you create your team, recognize and be able to explain that the most important concept underlying real-world security is the principle of least access: Shut everybody out of everything on your network unless they have a solid business reason to be granted access to it.

Your development team should be made up of people who work with your network and the Internet, but who come from different functional areas of the company. Each manager in your company has a unique view of the needs and risks. You need people who know something about the technology, but also some who know about business. Include some people from the trenches, too; there is nothing less useful than a painstakingly documented security policy that, when implemented, keeps the shipping department from being able to track packages, or blocks the sales reps from network resources while they are on the road.

1.2 How Secure is your System:

Try to determine which parts of your system are visible to external networks, modems, routers, remote access servers, Where are your important systems and configurations kept and how easy would it be for you to access them? How easy would it be for you to steal passwords? Could you hack them, or could you get them from employees? If you think like a hacker, you will unearth system weaknesses you didn't know existed.

The newest attacks are automated, requiring no human trigger to deliver their destructive payloads. The speed with which they can then propagate outpaces the speed with which any human can deal with them, introducing the need for automated assessment, and vulnerability management.

Effective security protects the critical points of your network. In today's networks those critical points usually consist of the network perimeter, network

communications, server content and system configurations, and individual desktops. Focus on your vulnerability levels in these areas and determine where you need to implement protection.

2.0 Internet: A security threat:

The other side of an Internet economy is that companies must expose parts of their systems to the public. A firewall can protect these open access zones by creating a secure perimeter around your network, and defining exactly what, and who, can get in or out of your network at any time.

When you select a firewall, keep in mind the features and screening methods you need. The size of your enterprise will also dictate the firewall you need to most benefit your business.

Since the Internet is a public network, any confidential information you send across can be intercepted at any of the devices it pass through. Encryption turns your words into code, with only authorized parties possessing the key to decipher it, protecting your confidentiality and the integrity of the information, and verifying the sender. Since this is like creating your own private area of the Internet, these systems are known as virtual private networks, and are much less expensive that using leased private lines.

VPNs allow businesses to take advantage of the Internet, and affordable broadband transmissions for secure, private communications. VPN technology can bring outstanding benefits to mobile users, branch offices, and extranets.

2.1 Virus: Downloadable from Internet:

The desktop can often be the weakest link in a defense system. Antivirus software is a must for protection against known viruses, Web attacks, and e-mail intrusions to desktop environments and infrastructures. Your antivirus software should be updated regularly to be most effective.

Now about countering the threat. Your top-level policy should state:

- What you are protecting and how you will go about it
- How policy changes will be managed
- Who has a voice in policy change

3.0 Steps towards Securing a Network:

Assign each policy section to an individual staff member; select a review group, and schedule reviews and deadlines. Your policy should be audited regularly, and undergo a thorough periodic review. Sitting down to write a database password policy isn't easy, but luckily you can find many free templates on the Internet.

The important steps you could take is:

Backup and storage are the foundation of your road to recovery after any security breach. Data backup can be to CDs or DVDs, and should be stored offsite. There are even companies that will manage your storage and backup for you.

Test your backups and make sure restoring from the backup media actually works.

Learn about logs. Routers, firewalls, Web servers, file servers, etc., all generate logs. Learn how to read them and recognize normal and abnormal traffic. Try to audit logs as consistently as possible.

Disable or remove all unnecessary services BEFORE connecting systems.

Change the passwords immediately upon installation. Never run systems using default passwords.

When new faults are identified, test and update your systems with appropriate patches as soon as you can. Remember that not all patches are created equal, and neither do they address equally severe issues. Use good judgment in deciding when to patch.

Consider encrypting all raw, unencrypted text before sending it across the Internet. Remember that e-mail is raw, unencrypted text.

Never give passwords over the phone without authenticating the individual.

Always examine new network devices and configure them before putting them into production.

Create passwords with one or more of the following characteristics: many characters, using numbers, letters, and punctuation; case-sensitive; no default passwords; no words straight from the dictionary. Make a point of protecting the repository where you store the passwords.

Protect password integrity with a comprehensive set of rules. Bear in mind that the more complicate the password scheme, the more time you will spend on support. It may be more cost-effective to procure third-party technology for password management.

Enforce user password changes every 60 days.

Change administrator passwords every 30 days.

Consider encrypting data on all laptops to prevent data theft should they be stolen.

3.1 Role of Organizational Staff:

Clear instructions and a guide to the complete security policy provide the framework for regulation. Remember that security training needs to be regularly administered and updated. Management should fulfill their obligation by providing on-the-job employee training that addresses security policy, procedures, and the company's business philosophy and priorities. Educate users on the reasons for the following restrictions and guidelines. Because the biggest obstacle to IT security policy is employee awareness, clear communications and training are two of the most crucial responsibilities you have in getting end users to help you secure your company assets. Internal security compromises arise primarily from unwitting actions and inconvenience, rather than fraud or malice. The staff needs to feel that a security policy is in their interest, not simply a scheme to raise the profile of the IT manager.

There is no single solution that cures every security problem. Today's network security requires a wide reach, including VPN, intrusion prevention, application layer inspection, antivirus, and content security. Yet none of these protections alone can do the entire job. To be effective, security solution tools must work together to secure the critical points of your network: the perimeter, your servers, your communications, and your desktop environments. These solutions must also be adaptable enough to easily incorporate new functionality to meet emerging threats.

You understand the importance of protecting your business against Internet threats. We hope this paper has given you some good tools for implementing a security solution you can use and trust. Once you have developed your security plan, we caution you to implement it very watchfully.

Correspondence to:

Jaya Prasad, ME, Comp. Sc., Professor
Officiating Principal, Professor and Head,
Department of Computer Science and Engineering
New Horizon College of Engineering, Bangalore, India
"Bonavista"
No: 653, 7th cross, I satge, V Block,
H.B.R. layout.
Bangalore – 43.
Emails: mj_prasad@yahoo.com
ravi8910@gmail.com
Phones: Office: 91-080 – 28440532.
Home: 91-080 – 25430842.
Cellular: 9449222809

Received: 1/5/2007