

# How Vulnerable Are Your Information Systems?

BY GIDEON J. LENKEY

Protecting your information systems from continuously emerging threats has become increasingly more difficult and expensive. This is despite the availability of a cornucopia of products ranging from anti-virus software through and including the latest generation of firewalls and intrusion detection systems. Information system security has been a well-documented problem for over 30 years. After using technology to abate a seemingly technological problem for such a long time with demonstrably diminishing results, one possible conclusion is that technology alone can't solve the problem, that there is no silver bullet product, service or device that will mean you no longer have to worry about information security.

The difficulty in dealing with information system security is that there are so many ways to access the information stored and processed. A would-be thief could get at it through the application, break into the operating system and take it, steal a backup tape or simply convince a system user to reveal it for a seemingly legitimate purpose. With so many ways to compromise your customers' data, you have to look very closely at and understand all of the possibilities. The goal is to look at your organization as a thief would. There are many types of thieves, so this effort has to consider everything from the janitorial contractor to the refined con man. You probably can't stop a truly determined thief, but you can raise the bar high enough to encourage him to find an easier target. During this process you'll find that with a better understanding of your security posture, you'll begin to understand your true security needs.

## Conduct a "VA"

It all starts with the vulnerability assessment or "VA" as it is known. A VA is the first step in a healthy security process, one that is ongoing and without end. Security of your information systems is not a destination you arrive at, rather it's an ongoing process by which you observe, plan and react to existing and emerging threats. As with anything you do repetitiously, a healthy process gets easier and less expensive over time. Turning what you learn from the VA into a plan and then implementing it are steps two and three of the process. These steps are beyond the scope of this article.

The goal of the VA is to discover and understand any possible way the confidentiality, integrity or availability (CIA) of your bank's infor-

mation may be vulnerable. During this process, you should not only consider the possibility of deliberate attacks, but anything that will affect the CIA of your information. For example, in one case I recall a data center that contained a large stack of cardboard boxes full of papers. The boxes were placed on and around a large power transformer. In the cool dry air of a data center, one spark could have resulted in a serious fire. A data center fire can be a catastrophic and financially devastating event that can certainly threaten the integrity and availability of your information.

This process is considerably different than a penetration test (PT). Although I've seen them used in a wider sense, a PT traditionally looks for a way into a specific application. As it is impractical to look forever, the test is usually time con-

The goal is to discover and understand any possible way the confidentiality, integrity or availability of your bank's information may be vulnerable.

strained for cost containment. The VA looks for anyway someone might be able to get at valuable information. A PT where no penetration occurs does not mean you're safe, it just means there wasn't a hole today. Tomorrow there could be a gaping hole. A VA looks to see if there is a hole, but also considers such factors as the process you use to patch systems and manage security devices. In this way a VA can tell you if you are likely to have a hole tomorrow. It's simply a more comprehensive and empirical view.

## A Comprehensive Assessment

A proper VA covers your organization from top to bottom, inside and out. If this sounds like a lot of work - it is. Areas to be examined include:

- *Internet Footprint:* The purpose of this ex-

amination is to determine what publicly facing, Internet addressable information system assets you have. These publicly available systems comprise your company's "footprint" on the Internet. While some footprint is necessary, an excessive footprint or particular configuration that allows an outsider to infer information about your infrastructure is certainly a liability.

- *Information Leaking Through Public Sources:* Some information about your organization is always publicly available. That is a part of doing business. The goal of this examination is to publicly find available information that may be useful to an attacker. For instance, a network administrator listed by name, office building number or telephone extension on the Internet domain registration record. This information can be valuable to a social engineer. Allowing him to impersonate a key network administrator for example.

- *Public Network Services:* Even if you only allow e-mail through your firewall into your corporate network, you are still offering a network service to the public Internet. How this service is configured can make all difference between being a responsible "netizen" (Internet citizen), a public nuisance or worse, facilitating the compromise of sensitive internal information.

- *Network Infrastructure Devices:* This examination looks closely at routers, switches, network printers and miscellaneous devices connected to or managed from your network. Many of these devices have network management interfaces that come from the factory enabled with default or no password protection at all. Imagine the damage if someone simply decided to set the IP address of one of these unprotected devices to that of your router, firewall or a critical system? It would effectively neutralize your network and possibly consume all of your IT resources. This would be a simple and effective distraction for someone with malicious intent. No special skills are required to mount this attack successfully, whether it is intentional or not.

- *VPN:* A properly configured virtual private network can greatly enhance your overall security. Improperly configured it can open gaping holes in your infrastructure. Password management, remote system configuration and physical security issues complicate effective use of this promising technology. An improperly configured VPN client can allow simultaneous network connectivity between the Internet and your corporate network effectively providing another way in for a malicious attacker. Cached passwords on a

portable computer present a serious threat if the device is stolen or misplaced. VPN technology being roughly equal, policy and procedure make the difference between an asset and a liability in this case.

•*Telephone Lines and Modems:* Most computers come with modems and almost everyone knows how to hook one up to a phone line. Any user on your network can install remote control software on their desktop and dial in from home with a minimum of knowledge. Some primary systems and even network infrastructure equipment have modems that are enabled and answering by default. Each enabled modem provides a potential point of access from the outside. By dialing every phone number and extension in the organization with special software, active modems can be located. More often than not, a company has more active modems than they are aware of.

•*Wireless Networking:* Wireless Networking protocols such as IEEE 802.11 offer the promise of easy installation and a quickly scaling network infrastructure. Unfortunately, the WEP encryption security scheme implemented in such devices is fatally flawed, however, this does not stop the proliferation of the technology. An attacker can be in a parking lot or building adjacent to you and gain access to your network as if wired up to it inside your building. An average user can easily install their own wireless access point without the help or knowledge of the network administrator or IT managers. This can inadvertently open your network to attack or misuse from the outside. Recently, new computers from major manufacturers come with wireless networking devices built in. A small software application, intentionally or maliciously installed, can activate the device and open your network up to a potential intruder. Wireless networking can be implemented safely and intelligently but must be checked regularly.

•*Desktop and Notebook Computers:* A lot of time and resources go into securing servers and critical information system assets. Desktop workstations and portable computers seldom receive such attention although these systems can have a profound impact on the overall security of critical information systems. Take for example the impact the Code Red worm had on corporate networks. Once inserted onto the corporate network through vulnerable Microsoft IIS servers the worm spread through other vulnerable Microsoft protocols. This worm had the effect of spreading so rapidly inside a corporate network that the resulting traffic essentially consumed all available bandwidth making the network unusable. Thoughtlessly implemented workstations, by virtue of their numbers, represent a potent weapon of mass disruption within your security perimeter.

•*Servers:* Are critical systems in default or insecure configurations? This examination looks closely at the purpose of the server in contrast to the network services it offers in addition to its security posture. For instance, an automated teller

central processing server does not likely need to provide POP3 remote e-mail service but it is often enabled with a default installation of the operating system. Every service offered to the network is a potential threat vector for attack. Only mission critical services should be offered and these services should be regularly maintained and scrutinized for configuration errors that can allow an attacker easy access.

•*Policies, Procedures and Practices:* The purpose of this examination is to determine how well the enterprise has adopted and implemented industry best practices. Policy is also closely examined. Written policy is frequently different from observed policy. For instance, although a policy of password rotation every 90 days is in effect, passwords over 200 days old are observed on critical privileged accounts. This is indicative of a wider problem that must be addressed managerially and enterprise wide.

•*Social Engineering:* How well your employees understand and react to social engineering attacks is of paramount importance to your organization's information security. People with access to information inside your organization can and

**F**or the VA to be an effective tool, it must offer recommendations that address the root causes of conditions observed in addition to any immediate remediation required.

do give it to people they haven't properly identified. Most of the time the employees victimized by social engineering "cons" are just trying to be helpful and efficient in their work. For instance, they think they are talking to someone who works at the bank in a difference branch or at the main office. A con man knows the lingo and often has scraped together bits of inside information by talking to various people throughout the organization over a period of time. By the time he's ready to execute his con, he sounds very convincing— after all he is a con man, it's what he does! The only defense is awareness and procedure.

•*Fire Suppression:* Often overlooked, fire suppression is vitally important to your information systems. Especially a data center where data processing equipment is at its highest concentration. Modern systems are effective if properly designed, installed and maintained. Unfortunately, errors in design or installation are not apparent until it's literally too late.

•*Physical access controls:* Physical access to critical systems can be an enormous advantage to a would-be attacker. Sometimes it's the most basic of failures that encourage an attacker. Improperly installed key-less entry systems, unprotected electric strikes and thoughtlessly placed motion activated exit switches all invite a physical intrusion. Backup tapes stored unlocked and in the open can also represent a serious risk. Why go through the trouble of breaking into a system, when you can switch a backup tape with a blank one and no one will ever miss it? It's always a good idea to walk the halls and try to see things from the attacker's point of view.

## Acting on the VA's Findings

The data collected during this effort must be carefully examined and considered. Root causes of inadequate security posture must be identified if effective permanent solutions are to be implemented. Solutions to poorly implemented security measures, servers in default configuration and written policy not enforced for instance, are often matters of training and process development rather than additional technical measures.

It's never enough to point out flaws or even reasons why something is flawed. For the VA to be an effective tool, it must offer recommendations that address the root causes of conditions observed in addition to any immediate remediation required. If you have a headache every day, your doctor is not going to keep giving you aspirin. He or she is going to want to find out what's causing it and focus on curing that.

A report needs to be written that summarizes the findings. This report should be relevant to upper management as well as IT technical staff. This means that it should have a non-technical summary as well as enough technical detail for the hands-on folks to do their work. A good VA report includes both recommendations as well as a suggested schedule for implementing them. In this way the VA can become vehicle for positive change.

Whether you perform your own VA in house or you contract it out to a security consultant, you should take the time to understand fully what the process entails. Don't accept a limited view of your posture by looking only at one or two areas. All of the areas described above are interrelated and you can miss the larger patterns of root cause if you don't consider them as such. The worst offender in this category is the stand alone "network scan," which is woefully inadequate at anything but creating a 10,000 item "to do" list.

Effective and permanent information security practice is a matter of understanding and addressing the root causes of poor security posture. Like a routine visit to the doctor for a check up, the VA is the way to make sure your network is security healthy and stays that way. ■

---

*Gideon J. Lenkey, CISSP is president and co-founder of Ra Security Systems in Whitehouse Station. He serves on the board of directors for the FBI's InfraGard program in New Jersey.*