

End-user Device Security

Tom Olzak
February 2005

Where does your business expend most of its resources to prevent malicious code attacks? If your company is like those for which I have worked, most of the time and effort is spent on the network perimeter and servers. But what about those ubiquitous end-user devices?

Desktop PCs, laptops, and Personal Digital Assistants (PDAs) are everywhere and usually connect to sites outside your security perimeter. In addition, more than 50% of your critical business information is likely stored on these systems (Sussman, 2004); they are also often the home for worms, viruses, and other malicious code. This makes end-user devices perfect portals for attacks against your network.

In this article, we explore many of the potential threats, vulnerabilities, and safeguards surrounding end-user computing.

The Problem

Every time a user connects to the Internet or any other network outside your security perimeter, the level of security on your network is affected. The points of concern in such a connection are depicted in Figure 1.

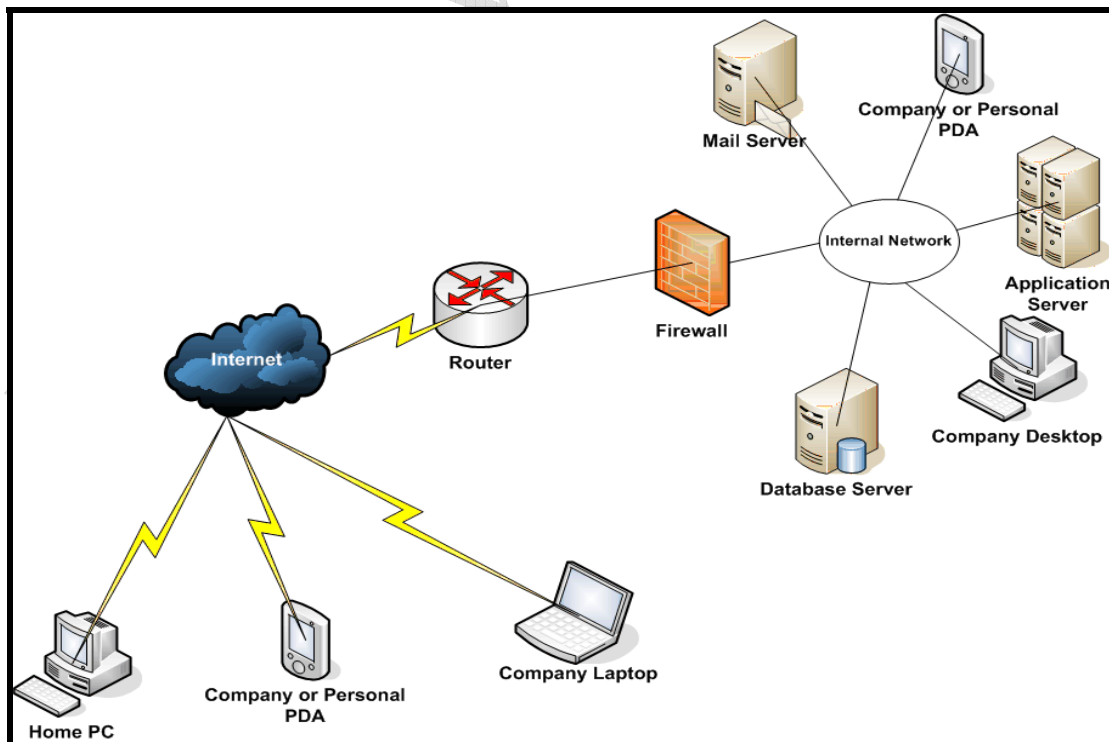


Figure 1: Common Network

Although my network engineering friends will tell me there are some pieces missing, this model is sufficient for our discussion. For the purpose of this article, I am assuming that the network in Figure 1 requires its remote users to connect to the company network over the Internet via a [Virtual Private Network \(VPN\)](#) connection. This configuration is becoming more common due to its greater flexibility and lower cost than traditional connectivity methods. The internal network is accessed through a [router](#) and a [firewall](#).

The Home PC, PDA, and laptop shown on the bottom left represent the plethora of external devices that may connect to your network and the Internet.

One of the biggest risks to networks today is the growth of end-user devices used outside the network security perimeter. Home PCs, PDAs, and laptops are becoming common tools used by employees to improve their productivity. However, the control most companies have on how, where, and when these devices connect is limited. These devices are commonly used to browse the Internet and connect to external networks over which you have no control. Couple these activities with a lack of consistent configurations, poor patch management, and outdated or absent antivirus software on both mobile and internal devices, and you create the conditions to bring your network to its knees.

So how can you protect yourself from these threats?

The Solution

Your [security program](#) should manage the threats caused by end-user devices with a layered approach. Figure 2 depicts a model for layered end-user device security.

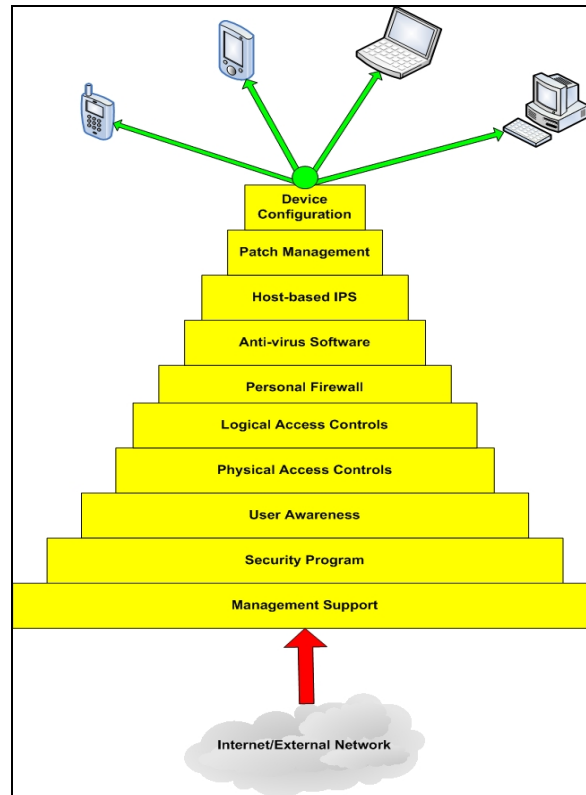


Figure 2: Layered End-user Security Model

The objective of end-user device layered security is to implement a variety of controls that, in their entirety, effectively neutralize incoming threats. Information moving from an external source to end-user devices at the far end of a layered security environment must pass through several different tests before reaching its target. These layers comprise administrative, physical, and technical safeguards. The effectiveness of this model must extend to all devices, whether located on the company network, at home, or at a customer site.

Is it necessary to implement all layers to ensure end-user device security? Not necessarily. Which layers to implement, and to what extent, is a risk management decision. To help with this decision, each of the layers is discussed below.

Elements of Layered End-user Device Security

Management Support

The foundation of any security program is management support. This support should be comprised, at a minimum, of effective policies, adequate budgets, and consistent enforcement. Efforts to change user behavior and to implement security measures carry no weight unless there is visible executive management support.

Security Program

An organization's security program facilitates the security objectives of management. It consists of policies and procedures.

Policies are high level statements of management's goals and objectives. They do not provide step-by-step directions to reach those goals and objectives; these directions are provided by procedures. A policy should consist of three elements:

1. Purpose
2. Scope
3. Compliance

The purpose of the policy clearly explains the objectives it is intended to achieve. It should also reflect management commitment to a secure enterprise. Scope describes all enterprise technology and activities affected by the policy. Finally, compliance defines consequences if the policy is not followed. It is the compliance piece – necessary to strongly encourage implementation - that is often missing from security policies.

Procedures are the administrative, physical, and technical recipes for producing a secure enterprise. They are derived from and support management policies. The step-by-step nature of procedures helps to ensure consistent compliance with security policy.

User Awareness

Unless fully engaged in the company's security efforts, end-users can be an organization's greatest threat. Awareness training, and related activities, is the best way to obtain end-user participation in a security program. Training should include:

1. Review of policies
2. Procedure implementation
3. Password protection
4. How to deal with [social engineering](#) attacks
5. Proper protection of workstations
 - a. Logging off before walking away from a device
 - b. Use of systems by unauthorized users
 - c. Elimination of potential [shoulder surfing](#) opportunities
6. Proper handling of PDAs, laptops, cell phones, etc.
7. Proper handling and disposition of media
 - a. Backup tapes
 - b. CD-ROM
 - c. Floppy disks
 - d. Other types of storage devices

Enhancing user awareness should begin with new hire orientation. Existing employees should receive the same training at least annually. In addition to formal training, daily reminders should be everywhere in the workplace; posters and login messages are two good vehicles for reminder distribution. Finally, first line managers must ensure that security compliance is part of every operational task.

Physical Access Controls

The effectiveness of the security program is directly proportional to the effectiveness of the physical access controls surrounding electronic information. Strong passwords, biometrics, and other logical access methods will not prevent the financial loss associated with the theft or physical destruction of critical business information. In addition, the level of effort applied to extracting information from secure devices within the normal business environment will probably fall far short of the effort applied in a [cracker's](#) basement.

Physical access controls include locked doors, cable locks, and security personnel. Also, educating users on the proper physical control of laptops, PDAs, and other mobile devices is an important factor in the prevention of information loss or compromise.

Logical Access Controls

Logical access controls prevent either unauthorized users from gaining access to any information resources or authorized users from gaining access to information for which they have no permissions. Logical controls include passwords, [biometrics](#), and [tokens](#). Regardless of the controls used, they should:

1. Have minimal impact on end-user productivity
2. Be reliable
3. Be effective with a ROI resulting from their initial and ongoing deployment costs

An analysis of the various logical access controls is beyond the scope of this paper. However, the following principles are provided as a guide:

1. Relying on strong, easy to forget passwords may be a mistake for your organization. Users often post strong passwords on their monitors or in other office locations that are less conspicuous but just as accessible.
2. Establishing an effective account policy is crucial to a logical access control implementation. The policy should include
 - a. Automatic password expiration, usually 60 to 90 days
 - b. A minimum password length
 - c. Password history to ensure that a password is not reused when it expires
 - d. A threshold of login attempts that when exceeded locks the user account, usually set at 3
 - e. An effective lockout duration that will deter [brute force attacks](#)

Finally, it is a good idea to combine password controls with another access control, such as biometrics. This is known as two factor authentication. If a password is compromised, the second control will help stop unauthorized use of system resources.

Personal Firewall

A personal firewall should not be confused with the hardware firewall that is commonly found on company network perimeters (see Figure 1). Rather, it is a set of related programs "...installed and administered on end-user devices to protect a single Internet-connected computer from intruders" (Noakes-Fry & Diamond, 2004). The personal firewall acts as the first logical line of defense against penetration attacks. Some of the functions performed by a personal firewall are:

1. To screen incoming traffic and block suspicious code
2. To screen outgoing messages that infect other company resources
3. To prevent the unauthorized use of logical [ports](#) by hiding them from malicious code or human penetration attempts

Although I have separated Antivirus and personal firewall software into two separate layers, most security software vendors provide solution suites that consist of both.

Antivirus Software

Malicious code attacks are the most common type of penetration into a company's internal network. According to the CSI/FBI 2004 Computer Crime and Security Survey, almost 40% of business losses related to security incidents are from virus attacks (Gordon et al, 2004). This was the number one cost, and it is well ahead of the second place cost, denial of service, at 18%. See Figure 3.

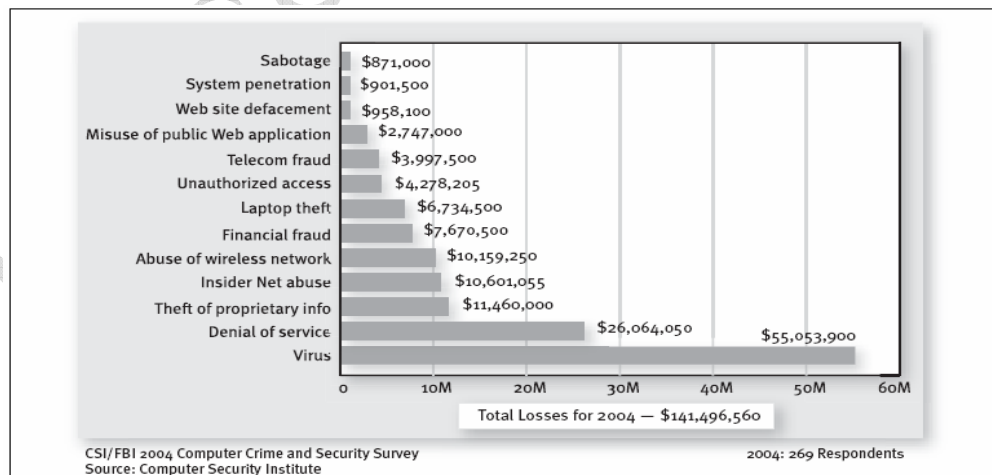


Figure 3: Security Incident Costs (Gordon et al, 2004)

Interestingly enough, the same survey revealed that 99% of the respondents list antivirus solutions as implemented within their enterprises. See Figure 4.

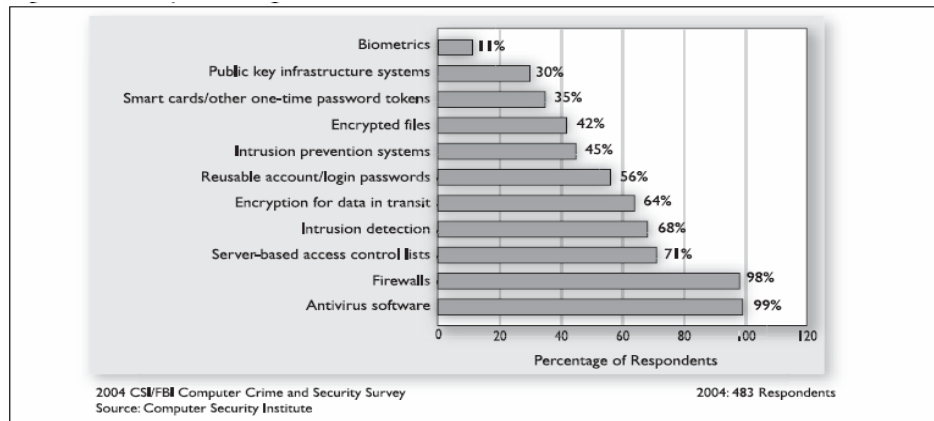


Figure 4: Deployed Security Solutions (Gordon et al, 2004)

Why, when nearly all of the 483 respondents to the survey have an antivirus solution in place did virus attacks move to the number one position? One explanation is the theory that target organizations often consider denial of service attacks as virus attacks (Gordon et al, 2004). Another cause may be the failure on the part of many organizations to maintain current [virus signature](#) files. Hundreds of new worms and viruses may be released each month. Without a consistent effort to keep antivirus solutions current and operational, every end user device in your network is a potential open door into your network.

Another point of entry may be home devices connecting to your network. Unless you implement a remote access solution that checks for the presence of an operational and up to date antivirus package, you are opening a gaping hole in your security perimeter. New technologies, such as [SSL VPN](#), provide the means to check for personal firewalls and antivirus applications before allowing a device access to internal resources.

But no matter how up to date you keep your antivirus solution, there is always a delay between the time new malicious code is identified and when your software vendor provides an update. You can fill this gap with Host-based IPS.

Host-based IPS

There are two primary types of Intrusion Protection Systems (IPS)- Network and host. Network-based IPS systems protect the entire network or a network segment. Host-based IPS systems reside on and protect individual systems. In this model, we focus on host-based systems.

In an ideal environment, malicious code and unauthorized users are always denied access to end-user devices. In addition, the protections in an

ideal environment prevent authorized users from destabilizing their systems as well as the network. But who works in an ideal environment?

Host-based IPS is a layer of protection that attempts to “catch” activities not blocked by the layers lower in the layered model pyramid. These activities include, but are not limited to:

1. Deleting files
2. Moving files
3. Copying files
4. Installing [executable files](#)
5. Registry modifications
6. [Denial of service](#) processes

Patch Management

Unless an end-user device is properly [patched](#), an attacker can take advantage of one or more of the many publicly known vulnerabilities in the end-user device environment. Organizations that delay the implementation of an effective patch management process may face increasing costs associated with attacks that exploit these weaknesses. “By 2006, software vulnerabilities caused by configuration errors will decrease, while attacks against newly discovered software flaws will increase” (Pescatore, 2004).

Figure 5 depicts the predicted increase in successful attacks associated with software vulnerabilities through 2006. Consequently, the use of patch management processes to eliminate software security flaws must be a critical component of any security program.

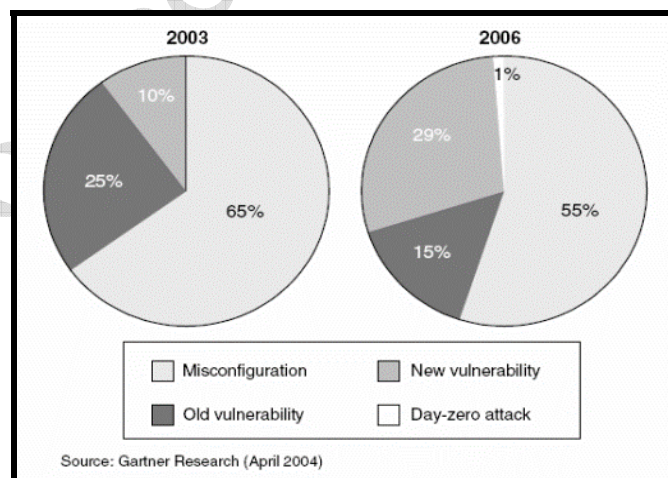


Figure 5: Increase in Successful Software Vulnerability Attacks (Pescatore, 2004)

Patch management, as referenced in our model, is a set of policies, processes, and tools employed to ensure that all end-user devices are at the proper patch level. Processes include:

1. Checking vendor resources for new patches
2. Checking end-user devices for current patch level
3. Applying patches to end-user devices

These processes can be very time consuming and expensive if done manually. Most organizations are prime candidates for one of the many automated patch management solutions available today.

Device Configuration

Taking another look at Figure 5, we can see that device configuration vulnerabilities will continue to be the number one target of malicious attacks. There are two primary paths to secure device configurations. First, we must continue to apply pressure on software vendors to distribute applications in “secure mode”. In other words, when I install an application it should install in a secure state. All services and add-ons that allow potential network or malicious code access to my application, even if it is an operating system, should be disabled by default.

The second path relies on each of us to securely deploy applications that may not yet support a secure state installation. This is sometimes known as “system hardening.” Some of the areas an organization should address include:

1. Keeping business applications and operating systems at the most current version. This provides not only the ability to take advantage of new security features; it also ensures the availability of security patches.
2. Ensuring that all devices require end-user [authentication](#).
3. Ensuring that remote access for the purpose of administration or support is controlled by strong authentication methods.
4. Shutting down any [service](#) that is not required for proper operation.
5. Controlling device configurations through the use of standard system images that are locked to prevent modification.
6. Using the security features included in the operating system to restrict access to information.
7. Ensuring systems are properly configured to perform backups.

Putting It All Together

Each of the layers in this model supports the layer below it. It is the implementation of different safeguards at each layer that provides effective protection. Is it necessary to implement all the layers? Not necessarily. What to implement and how much to spend on implementation is a business decision; a business decision that should be based on the results of a risk assessment.

A risk assessment takes into account the potential threats to the device, the vulnerabilities of the device, and the business impact in dollars of a security incident directed at the device. The following formula defines the relationship between these risk elements:

Risk = Threats X Vulnerabilities X Business Impact

The resources applied to minimizing risk should be proportionate to the level of risk. Resources should be applied to reduce one or more of the risk factors as close to zero as possible. So what is the best approach to mitigating risk?

Threats will always exist. Organizations have little control over this factor. Business impact is relatively static. There are, however, many opportunities to eliminate or mitigate vulnerabilities. The effective implementation of the layered model will result in reduced risk by eliminating or reducing end-user device vulnerabilities.

It is unreasonable to expect that any organization can completely eliminate losses due to security incidents. But the reasonable and appropriate application of a layered security model should help reduce risk to an acceptable level.

Copyright 2005 Thomas W. Olzak. Tom Olzak, MBA, CISSP, MCSE, is President and CEO of Erudio Security, LLC. He can be reached at tom.olzak@erudiosecurity.com.

Works Cited

- Gordon, L. A., Loeb, M. P., Lucychyn, W., & Richardson, R. (2004). *2004 CSI/FBI computer crime and security survey*. Retrieved January 22, 2004 from <http://www.qocsi.com/>
- Noakes-Fry, K. & Diamond, T. (June, 2004). *Personal firewalls: technology overview*. Retrieved December 19, 2004 from <http://www.gartner.com>, Document G00121188.
- Pescatore, J. (May, 2004). *CIO update: stay ahead of changing software vulnerabilities*. Retrieved December 19, 2004 from <http://www.gartner.com>, Document G00120818.
- Sussman, S. (March, 2004). Protecting corporate workstation and mobile system data. *Storage Networking World Online*. Retrieved December 19, 2004 from http://www.snwonline.com/evaluate/protecting_workstations_03-22-04.asp?article_id=374