

## Small Business Computer Security

By Bruce W. Roeckel

<http://www.immaculatetechnology.com>

### Four ways to secure your company on a shoestring budget

#### 1. Update and publish your security policy.

The weakest link in many organizations' security perimeter is employees. Therefore, it's important that workers be aware of what they're permitted—and not permitted—to do with their workstations. Security policies address this issue head-on by defining the boundaries of acceptable behavior.

Part of an organization's security policy should be its Internet acceptable-use policy. Here are some of the main points that should be included:

- Don't open e-mail messages from unknown or suspicious persons, or suspicious e-mail messages from known persons. Many viruses have been known to spread because of their enticing subject lines.
- Don't share access to computers or applications with other employees, and don't use other employees' access: Get your own. Anyone who requires additional access to computers or applications should make a formal request to the person or group that administers access.
- Use locking screen savers and lock your workstation when you leave your desk.
- Don't use the Internet at work for non-business-related purposes. This includes personal e-mail or Web surfing. Most organizations permit occasional exceptions.
- Don't install programs that are not approved by the IT department. Unsupported programs can not only jeopardize the stability of one's PC, but they also introduce undesirable programs such as spyware into the business network.
- Be very careful when allowing personally owned computers to connect to the business network, especially through an approved VPN program. Personally owned computers often lack up-to-date antivirus software and other protections. Require employees to maintain their personal systems with a minimum standard of protection.

# Immaculate Technology

---

Make sure employees are keenly aware of these rules. Here are a few ideas for ensuring that the word gets out:

- Hold mandatory security-awareness training classes.
- Get senior management's support for these policies, and have the CEO or chief operating officer send out e-mail(s) drawing employees' attention to these policies.
- Include a rule that states that failure to comply with policies will result in disciplinary action up to and including termination of employment.

## **2. Protect the *entire* perimeter, including laptops.**

If your organization has users with laptops, you can bet that some of them are connecting to the Internet via broadband connections (DSL, cable, satellite) lacking firewalls. This is exposing your laptops to the full force of still-active worms such as Blaster, Nachi, Slammer, Nimda and Code Red. A laptop whose antivirus signatures are not up to date and is connected to a broadband connection for any appreciable length of time *will* become infected with one of these worms.

Then, if the user connects the laptop to the corporate network—whether via VPN, RAS or on the premises—the laptop will begin scanning the network for more victims. Even if the rest of your systems' antivirus software is up to date, the effects from the scanning traffic alone is often enough to take down business-critical applications.

Don't permit contractors, temps, consultants or vendors to connect their laptops and other TCP/IP-enabled devices without approval from IT. You would be surprised by how many people—especially consultants and temps—still don't have any antivirus software on their laptops. Don't have a process? Make one, and quickly, that looks something like this:

- User or manager calls IT help desk with a request that IT examine a third-party device that he wants to connect to the network.
- IT sends a PC technician to examine the device for up-to-date antivirus software and signatures.
- If the device has working antivirus software, it will be permitted to connect to the network. If not, the device's owner will be required to acquire and install antivirus software.

Later, if a third-party laptop or other device is suspected of being infected with a worm or virus, IT can check its records to see if the person or department responsible made a request to have the device examined before connecting it to the network.

### **3. Block risky attachments on e-mail servers and gateways.**

A significant portion of Trojans and viruses are transported via e-mail. Even if your mail server has antivirus software, it would be prudent to strip certain attachment types from incoming e-mail messages, including .exe, .bat, .reg, .vb, .vbs, .com and .pif. For a list of selected attachment types to block, refer to information available from most antivirus software vendors.

You would be considered a good Netizen if you also blocked these attachment types in outbound messages, thereby halting the spread of a Trojan or virus. There is, by the way, a growing legal basis for preventing malicious code such as Trojans, viruses and worms from leaving your organization: You could be sued for damages related to your organization's permitting malicious code to penetrate your network and then spread to another.

### **4. Develop a security architecture, standards and requirements.**

Assemble a team of senior technologists to develop long-range objectives. First, take a look at your organization's current enterprise architecture and standards. Underneath all of this you should be able to develop a security architecture that provides common authentication services, as well as other "public utilities" such as central audit and event logging, and encryption of network traffic between servers.

When you get an idea of what your security architecture is going to look like, you can then take a shot at developing product and protocol standards. In each category of need, specify which product or protocol will be used. For instance, you might state that each desktop system will use Norton AntiVirus software and no other. For encryption of application and administrative traffic between systems, you could use IPsec. Do this for each area where a product, protocol or method is needed to fulfill a particular purpose.

Develop a boilerplate requirements document that will be given to all software and hardware vendors, and also to internal systems developers and integrators. These requirements define how information systems must behave and what protocols and standards they must support. This will streamline the adoption of new products into your infrastructure by make them more consistent with what you already have.

These measures will save your organization money in the long run by reducing implementation and operating costs. A more consistent infrastructure is less expensive to maintain.