CONTRIBUTORS

IN-FIRM Security Tips

Column: Technology IN Practice

Aug. 01, 2007

From the August 2007 Issue

Virtually every week there is another headline about a major security breach of digital data. What would be the impact to your firm's reputation if it were the victim of such an attack? Security today is very serious business, but it is an area that tax and accounting firms tend to downplay or assume is being properly handled by internal IT resources. In most firms, the IT team is understaffed and focused on keeping the network stable, which takes all of their time. Seldom do they have adequate training to be aware of today's security threats, let alone ensure that the network is properly protected against those threats. For this reason, I recommend that ALL firms outsource all the upper-level security requirements to an external IT organization with specialists on staff whose sole role is to keep up with security issues and to develop a security routine to make sure the firm is protected.

Independent Security Audits

Firms should consider having an independent third party conduct a security audit whenever they have implemented new servers or made any significant change in their Internet connectivity. I recommend that this be a different group than the external network integrator the firm utilized to install the network, and they should have a person on board that specializes in security so you truly get an independent review. While all "one shot" security installations

should be outsourced, there are maintenance items that internal IT personnel should monitor regularly, which I've outlined below.

Viruses

According to the CIS/FBI 2006 Computer Crime and Security Survey, viruses caused the greatest amount of financial losses to businesses, so it is imperative that the firm utilize an antivirus application that is reliable and updated frequently. Today, I recommend that firms stick with one of the major providers such as Symantec/Norton, McAfee or Trend Micro. Most firms originally set the default to update its virus footprints on a daily basis. Today, these settings should be updated to provide automatic notification when an update is available or to check at least on an hourly basis. To add an additional layer of antivirus security, many firms are now going to e-mail management companies such as Postini,
BrightMail and AppRiver to do enterprise class antivirus filtering along with their spam management services, prior to delivering e-mails to the firm, which can create two-layer protection against viruses and other malware.

Spyware

Spyware is another type of malware that can impact the performance of computers, and it is recommended that firms have at least two products at their disposal. In addition to the industry favorites of WebRoot SpySweeper, AdAwareSE, and SpyBot Search and Destroy, Microsoft has rolled out its own Windows Defender product that has proven to be effective. Firms should have a process in place to verify that workstations regularly have their virus and spyware "footprints" updated and that these workstations are scanned.

Unauthorized Access to Firm Data

Another primary security threat to firms is the ability for unauthorized personnel to access the firm's data through its Internet connection. While virtually all firms have a firewall in place, the installation and maintenance can still leave the firm unknowingly exposed. To see if your firm's firewall has been certified by today's standards, ICSA Labs (www.icsalabs.com) maintains a database for this purpose. It is also important to have your firewall checked regularly to ensure that no changes have been made without the firm's awareness. One easy-to-use service is ShieldsUp! from Gibson Research Corporation (www.grc.com). This utility will scan the first 1,056 Internet ports and let you know if those ports are open, closed or in stealth mode. The firm's network administrator can run this test regularly as part of an IT flash report

to compare to previous results and help determine whether or not to contact the firm's security support group.

Current Network Operating System

Not keeping your network operating system current is another security risk to firms. Each year, the SANS top 20 (www.sans.org) lists the most critical Internet security vulnerabilities, most of which can be protected against by having the current network operating patches loaded. To see how well your firm is protected against the top 20 vulnerabilities, which account for the vast majority of breaches, Qualys (www.qualys.com) has a utility that you can download and run against your systems. In addition, as most tax and accounting firms utilize the Windows network operating systems, firms can download Microsoft's Baseline Security Analyzer, which is an automated tool that evaluates your current security status as well as recommends which patches you should install. Implementation of patches can be further automated with Microsoft's Windows System Upgrade Server to notify the firm's IT personnel as soon as new updates and patches are released.

Access Controls

Access controls are another area where firms are notoriously lax. This begins with the building's security code. Ideally, each person would have their own access code, which could be terminated with the employee. For firms that only have one security code for all personnel, it is important to change that whenever there is a change of personnel or of maintenance service providers. Another access code is the individual passwords of firm personnel, which should be changed at least twice per year with rules enforced by the network operating system. Today, it is recommended to have at least eight characters that contain case sensitive alphabetic, numeric and character symbols to make them hard to guess. For a sample password policy (and other computer usage policies), SANS (www.sans.org) provides them on its website.

Computer/Internet Usage Policies

Finally, it has often been said that people are the weakest link in the security arena, so it is imperative to make them aware of security threats and keep them updated on firm computer policies. It is recommended that firms have a computer/Internet
usage policy in place that is reviewed annually to make sure it covers today's technologies such as wireless and remote access, PDA usage, and threats like pharming and phishing, as well as how to respond to a security situation. Scheduling

an hour annually to educate firm personnel will help keep them informed and better protect the firm.

Conclusion

Security of firm information resources is everyone's responsibility. To optimally protect the firm will require a combination of internal and external technical resources as well as education and awareness of all firm personnel. Act today to minimize your firm's risk in the future.

Contributors • Roman Kepczyk • Article

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.