How Safe Is Safe Enough?

Protecting your firm's and your clients' data

08/01/2014
AccountingToday.com
By Dave McClure

In September of 2013, security for small accounting offices changed forever with the appearance of a new class of threats called ransomware.

It began with CryptoLocker, but that program was quickly followed by CryptoBit, then CryptoDefense and, most recently, Kovter. All of them work basically in the same way -- you open a file attached to an innocent-looking e-mail, and the program encrypts key files and drives so they cannot be accessed. The files are locked until you pay a ransom. The longer you wait to pay, the higher the ransom required. Kovter goes a step further - it places child pornography on the computer before the drive is encrypted. Traditional defenses such as anti-virus programs and firewalls are virtually useless against this new threat.

"Anti-virus programs are more critical than ever before, but also more useless than ever before," said David Cieslak, principal at accounting technology firm Arxis Technology Inc. "Malware today is able to get underneath even the best anti-virus programs. What's more, the infected machine can operate in a compromised state for weeks or months without the user being aware. The malware operates in stealth mode, so accountants think their machines are okay and in good working order, while in fact they are not."

"What we are experiencing is that the attacks on small businesses are more robust than ever before," Cieslak continued. "You can't hide by being small, because the attacks are so automated. Some of the least protected systems are in small businesses. You can't let your size trick you into thinking you are safe."

"Traditional legacy solutions like firewalls and anti-virus programs still have their place," said Jerry Irvine, chief information officer of Prescient Solutions and a member of the National Cyber Security Task Force. "But it is no longer a zone protection strategy. These traditional defenses need to be part of an application defense based on that data that includes access controls, application firewalls that are intelligent enough to recognize [a threat] as it comes in, and defenses that work on the enterprise level. That is the future."

"It is a matter of following security best practices," said Randy Werner, an attorney and CPA who serves as a loss prevention executive for Camico. "Small firms tend to hang on to a lot of data, perhaps far longer than they need to. This data still contains personally identifiable information about clients, and if you are hit with a hacker attack, you could be found to fall below the standard of care from a risk and liability standpoint."

This has not escaped the attention of regulators, who have placed some significant requirements on financial services firms, including accounting firms and tax preparers. (*See "Overprotected?" below.*)

BEST PRACTICES

Accounting firms face special security challenges that other small businesses don't contend with. Because of the data they collect for tax, payroll and other services, they are priority targets for hackers and identity thieves. In some cases, data must be retained for a period of years for historic comparisons, requiring more extensive protection strategies.

There is no shortage of lists of "security best practices" from government agencies, security product vendors and independent security and risk management professionals. But these are often of little value to accounting firms that do not have an internal IT staff. They are hopelessly complicated, require a massive time commitment from the owner or partners, and are too costly to implement.

What is needed is a simpler approach to security -- an approach that makes the best use of available technologies, balances risk versus resources, and effectively protects both the firm and its data. Here is what accounting security professionals recommend:

1. Do the obvious. There are some things that we all know should be done, but that can get lost in the desire to serve clients. If you are still running Windows XP, upgrade to Windows 8.1. Set all computers to automatically install security patches from Microsoft, even during tax season. Keep the server firewall in place and the anti-virus program up to date. Set the anti-virus program to sweep the entire network on a regular basis. Back up all data at least daily, if it is necessary to retain data on the premises. Ensure that passwords are used on all computers, and that these are changed on a regular basis. Do not use the same password for the network and external Web sites.

2. Physically secure the network. Though the majority of security threats will come from outside the network through remote connections or e-mail, it is still possible to lose data if the network is physically breached. Keep the office server in a locked cage with appropriate backup power and ventilation. Set access controls so that only those with a need for it have access. Use software locks for all mobile devices, and additional physical locks on all laptops. Control access to the office through key system management, use an alarm system, and install security cameras in critical areas.

3. Set a security policy and enforce it rigidly. Remember that users of the network are its weakest link, and that a single careless moment by any member of the firm can bring the business to its knees through data theft or ransomware. Among the things that should be addressed in the policy are the purpose of the policy; internal access control to computers and servers; a ban on use of personal software on office computers; a ban on temporary storage devices such as thumb drives; a ban on opening attachments to any e-mail; limited access to Web sites; termination and retirement procedures; and procurement policies for computer equipment and mobile devices. While it may seem harsh to limit access to the World Wide Web, personal

software and personal devices, remember that these are a major potential threat to the security of the client data.

4. Use a secure portal for all client communications. Portals allow for secure communications between the accounting firm and the client, as well as secure storage of documents in transit. Every major accounting and tax software vendor now offers a client portal service specifically designed for the needs of the industry. Not using a portal is to risk a violation of the law, with attendant fines and penalties.

5. Move to the cloud. There are obvious advantages in lower IT costs for the firm, as well as having updates and enhancements applied automatically. In addition, the use of cloud services for software, services and file storage enables anytime/anywhere access. That said, consumer cloud services are not appropriate for accounting files. Perform due diligence on the cloud provider, even those that are known vendors to the industry. Look for cloud storage providers, for example, that are PCSI- (payment card) and/or HIPAA-certified. In addition, look for providers that have a Service Organization Control 2 or SOC 3 attestation report. (For information about these reports and their relevance, visit the AICPA Web site.)

6. Adopt end-point security. As previously noted, defensive systems built around protecting the server with a firewall and anti-virus program alone are over, as attacks against the network have become too sophisticated for these to provide enough protection. Instead, security vendors are increasingly stressing a more heuristic, end-point security strategy. End-point security aims to protect the data by managing remote access to the network. It requires each computing device on a corporate network ("end-points") to comply with certain standards before network access is granted. Endpoints can include PCs, laptops, smart phones, tablets and specialized equipment such as bar code readers or point-of-sale terminals. The precise services offered as "end-point security" may differ from one vendor to another, but generally combine legacy firewall and anti-virus programs with anti-spyware and intrusion detection systems.

7. Lock down the e-mail system. E-mail is one of the weakest links in the network, and one of the two major ways malware gets in. All e-mail communications should be encrypted, even though encryption is not foolproof. In addition, the firm should enforce a policy of never opening attachments for any e-mails -- if a document needs to be transmitted, the client portal or cloud storage system should be used for this purpose. This may be one of the more difficult policies to enforce, but also the most important.

8. Clean up local data storage. Many accountants are data packrats, maintaining client files in the office for far longer than they are needed. Retain only the data that is actually needed and move it to the cloud for secure storage. The rest should be archived in longer-term storage where it is still accessible but is kept safe.

9. Communicate your security strategies to clients. No data security system can be truly successful unless clients understand what you are doing and why. In this age of identity theft, clients may also see your commitment to security as a strong point in your favor. As you meet with each client for other services, make a point of the changes being made to the firm's data protection systems.

10. Get expert help. Once the basics have been covered -- policies, strategies, portals, cloud storage, e-mail lockdown and communication -- consider calling in the experts to take the next step. Experts in accounting security can help with more advanced defenses that include application scanning, port scanning, vulnerability scanning and penetration tests, with recommendations on how to handle any weaknesses that are identified. In addition, because these professionals keep pace with changes in the industry on a daily basis, they will be able to help the firm keep current on emerging threats.

These 10 best practices for securing accounting data form the outline of a basic plan, and will provide the first layer of protection in what will ultimately become a multi-layered defensive strategy. Those layers combine strong technologies with strong procedures.

"The state of the art are the applications that scan data as it comes in," said Prescient Solutions' Irvine. "This means that each piece of data is scanned for patterns that are inconsistent, using applications that are intelligent enough to recognize the data coming in."

"Successful breaches mostly come from people clicking on infected links," said Arxis Technology's Cieslak. "It may come in the form of compromised Web sites or e-mail, but ultimately it is someone clicking through that puts the firm at risk. People, not systems, are the weak link in the network."

"You have to raise the level of sophistication of both users and clients," agreed Camico's Werner. "Both need to be trained to make data protection a priority. This will take time, effort, patience and management attention, but is critical to the long-term survival of the firm."

OVERPROTECTED?

Accounting firms, regardless of size or type ofpractice, are required to meet a wide array of legal standards:

- **Circular 230.** According to the Internal Revenue Service, in its publication Safeguarding Taxpayer Data, protecting this data is a top priority for the IRS, as is reflected in Circular 230. Best practices outlined in the safeguarding document include locking doors to restrict access to paper or electronic files; requiring passwords to restrict access to computer files; encrypting electronically stored taxpayer data; keeping a backup of electronic data for recovery purposes; and shredding paper containing taxpayer information before throwing it in the trash.
- **The Gramm-Leach-Bliley Financial Modernization Act of 1999.** Known as the Gramm-Leach-Bliley Act, this directed the Federal Trade Commission to establish the Financial Privacy Rule and the Safeguards Rule. It also extended the definition of financial institutions to include financial planners and tax preparers.
- **The FTC Standards for Safeguarding Customer Information Rule (16 CFR Part 314).** Also known as the Safeguards Rule, this requires financial institutions - as defined to include professional tax preparers, data processors, affiliates, and service providers - to ensure the security and confidentiality of customer records and information. It protects against any anticipated threats or hazards to the security or integrity of such records. In

addition, it protects against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

- **The Financial Privacy Rule.** This aims to protect the privacy of the consumer by requiring financial institutions to give their customers privacy notices that explain the financial institution's information collection and sharing practices. In turn, customers have the right to limit some sharing of their information. Also, financial institutions and other companies that receive personal financial information from a financial institution may be limited in their ability to use that information. The FTC Privacy Rule implements Sections 501 and 502(b)(2) of the GLB Act requirements.
- **Title 26: Internal Revenue Code (IRC) Â§ 301.7216.1.** This imposes criminal penalties on any person engaged in the business of preparing or providing services in connection with the preparation of tax returns who knowingly or recklessly makes unauthorized disclosures or uses of information furnished to them in connection with the preparation of an income tax return.
- **Title 26: Internal Revenue Code Sec. 6713.** This imposes monetary penalties on unauthorized disclosures or uses of taxpayer information by any person engaged in the business of preparing or providing services in connection with the preparation of tax returns.
- **Internal Revenue Procedure 2005-60.** This requires authorized IRS e-file providers to have security systems in place to prevent unauthorized access to taxpayer accounts and personal information by third parties. It also specifies that violations of the GLB Act and the implementing rules and regulations promulgated by the FTC, as well as violations of the non-disclosure rules contained in IRC Sections 6713 and 7216, are considered violations of Revenue Procedure 2005-60, and are subject to sanctions specified in the revenue procedure.
- **Additional state and local laws.** States including California, Connecticut, Maryland, Massachusetts, Nevada, Oregon and Rhode Island have enacted laws requiring businesses to maintain data security standards to protect state residents' personal information from being compromised. The Massachusetts data privacy regulations are among the most comprehensive of the state data security laws. The state's regulations go beyond most other state data security laws by requiring every "person" or entity -- including businesses both inside and outside of Massachusetts -- holding, processing or otherwise accessing personal information of Massachusetts residents, to develop a comprehensive written policy outlining their physical, administrative and technical information security measures; to maintain extensive computer system security requirements; to encrypt all records containing personal information transmitted over wireless networks or stored on portable devices; to require third-party service providers (e.g., payroll providers, outsourcers, etc.) receiving personal information, by contract, to maintain security measures in compliance with the regulations; to train employees on compliance with data security policies; and to regularly monitor and review security measures, at least annually, to ensure that they are preventing unauthorized access to personal information.