How to Improve Your Defenses Against Two Common Cyber Threats

By Lisa Traina, Partner

In a recent survey, 63% of nonprofits reported having at least one data breach in the prior year.* With new threats unleashed almost daily, that percentage will only grow.

There are many different ways your network and data can be breached, from malware to sophisticated ransomware attacks. Two of the most prevalent cybersecurity threats, however, are vulnerabilities and phishing. Let's look at the risks posed by each and steps your organization can take to reduce those risks.

Vulnerabilities: Software Holes that Open the Door to Hackers

In March 2018, the City of Atlanta was the victim of a ransomware attack that encrypted data and led to the shutdown of some city services. Weeks later, many departments were still without access to critical data. The attack is believed to have been caused by ransomware that relies on a vulnerability in Java-based servers.

Likewise, the May 2017 WannaCry ransomware program exploited a vulnerability to launch more than 75,000 ransomware attacks in 153 countries. Victims could have prevented the attack by installing a Microsoft update that had been available for two months.

Vulnerabilities, like the ones used these attacks, are holes in software code that hackers can use to gain access to a system. Vulnerabilities can exist in all software, including operating systems and applications. They are closed by applying patches and updates.

95%

of phishing attacks that led to a breach were followed with some form of malware

The most common vulnerabilities identified in the testing we perform for clients are:

- Missing patches or outdated software (this is the vulnerability we see most frequently)
- Misconfigured web servers and other devices
- Open interfaces the client wasn't aware of, such as an admin portal to a firewall, internal server, or shared folder on an internal computer

To help reduce your organization's risk from vulnerabilities:

- Consistently patch and update all systems
- Perform regular vulnerability scans of your internal network and external Internet-facing systems to uncover any existing holes
- Create and implement a zero-day vulnerability plan to address vulnerabilities for which no update or patch is yet available

Phishing: Fraudulent Communications Targeting Human Error

Hackers craft these fraudulent emails to entice the recipient into an action that gives the hacker access to a computer system or sensitive information.

A phishing email might trick a recipient into wiring funds in response to a request that looks like it's from their CFO, for example, or lead the recipient to click a link or attachment that installs malware on their computer.

Phishing can take many different forms, from typo-ridden emails to legitimate-looking communications that appear to be from a trusted source. And unfortunately, phishing is very effective. According to Verizon's 2017 Data Breach Investigations Report:

- 1 in 14 users were enticed into clicking a link or attachment in a phishing attempt
- 25% took the bait a second time

- 95% of phishing attacks that led to a breach were followed with some form of malware
- 28% of phishing breaches were targeted

Take these steps to help reduce your organization's risk of a phishing attack:

- Educate all employees on how phishing attacks work and the signs to watch for
- Tighten up your email security, such as by using multi-factor authentication
- Be aware that phishing emails can get through even the best filtering systems
- Check that the controls you have in place are working as intended

Assessing and Improving Your Organization's Cyber Health

As the statistics above illustrate, just one unaddressed vulnerability or one employee's click on a phishing email can lead to a breach of your network. A breach can result in disrupted operations, financial loss, and damage to your organization's reputation and trust.

The Cyber Checkup from CapinTech is designed to help you check and improve your organization's cyber health in these two high-risk areas. It consists of:

- External Vulnerability Scan – We use proprietary software to scan your network against a database of more than 50,000 known vulnerabilities. This identifies vulnerabilities that can be seen and exploited from the public Internet.
- Phishing Test – We will perform a social engineering test to help determine your employees' ability to identify fraudulent email. You can use the data to implement effective employee training.

At the completion of the Cyber Checkup, you'll receive a report of our findings and recommendations to help you determine next steps. This service can provide you with a clear analysis of your organization's cyber health in these two important areas, and action items to help you improve it.

Strengthening Your Defenses

The most important thing to keep in mind is that all organizations, of all sizes, are at risk of a cyber attack. While the threat is significant, implementing the right processes and controls can help reduce your organization's risk.

Please contact us at cybersecurity@capincrouse.com with any questions or to learn more about the Cyber Checkup.

About the Author

Lisa Traina, Partner
CapinTech
ltraina@capincrouse.com
o 505.50.CAPIN ext. 2000

Lisa uses her more than 30 years of experience to assist organizations in implementing measures to secure data and manage risks efficiently and effectively. She is a nationally recognized speaker and author, and serves on the AICPA Cybersecurity Task Force. Lisa founded Traina & Associates in 1999 to provide IS security services to a broad range of industries. Traina & Associates joined CapinCrouse in January 2017 and is now CapinTech.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA

*2016 Compliance Effectiveness Survey, The Society of Corporate Compliance and Ethics and the Health Care Compliance Association, accessed April 4, 2018