STRENGTHEN YOUR COMPANY'S DATA SECURITY THROUGH PROACTIVE TESTING

WISS

A Partner to Grow With

Information provided by Wiss & Company in this document is intended for reference only. The information is designed solely to provide guidance, and is not intended to be a substitute for someone seeking personalized professional advice based on specific factual situations. Although Wiss & Company has made every reasonable effort to ensure that the information provided is accurate, Wiss, and its partners, managers and staff, make no warranties, expressed or implied, on the information provided. The reader accepts the information as is and assumes all responsibility for the use of such information.

By taking a forward-thinking approach to data security threats, we can minimize risks and maintain a stable and secure network for our clients

Wiss & Company's clients entrust us with their financial information and other sensitive data, and we take that responsibility seriously. We've invested significant time and resources in advanced technology to safeguard data and protect against external security threats. We also use our expertise in this area to help other companies improve their data security and minimize threats.

DATA BREACHES – A GROWING THREAT

Hackers, or data thieves, present a tremendous – and growing – threat to organizations with highly sensitive data. Data theft is on the rise, impacting companies of all sizes and across industries; in 2013 alone, the IRS paid out more than $5.8 billion in fraudulent refunds instigated by hackers.

Examples of recent highly visible data hacks include:

November/December 2013: Target

Data thieves stole the personal identification data of 70 million customers during the height of the holiday shopping season. Exposed information included names, mailing addresses, phone numbers and email account data, as well as credit and debit card numbers, expiration dates, three-digit CVV security codes and even PIN data.

July 2014: JP Morgan Chase

The loss included 76 million names, addresses, phone numbers and email addresses.

September 2014: Home Depot

Hackers secretly embedded malware on cash registers in 2,200 stores, enabling them to steal sensitive data from 56 million credit and debit card transactions.

November 2014: Sony

Culprits leaked insider information from Hollywood studios, including unreleased film, sensitive emails, password data and executive salary information.

February 2015: Anthem

The names, personal addresses, Social Security numbers and email addresses of 1 million members were stolen.

June/July 2015: United States Office of Personnel Management (OPM)

OPM announced it had been hit by a data breach targeting the records of as many as 4 million people. By early July, the estimated number of records stolen jumped to 21.5 million.

Who's next?

> Think of penetration testing as testing the locks and alarms that prevent access from unauthorized parties, employing a highly trained independent third-party security company

PEOPLE, PROCESSES AND TECHNOLOGY

How can organizations increase network security and be confident that their information is protected? At Wiss, we've found the most effective strategy is to pay careful attention to people, processes and technology.

Our company for years has invested in network security solutions such as advanced firewall protection, encrypted hard drives, encrypted pen drives, McAfee Antivirus/web content filtering and annual perimeter penetration testing. Two years ago, we increased our investment by moving all mission-critical applications and data to an outside data center, which provides enhanced security at its SSAE 16 SOC 1 Type 2 redundant facilities.

Migration to the data center gave us confidence that we had the right technology in place for network security. But while we'd become increasing effective at protecting our systems from outside threats, we knew that no organization can afford to become complacent when it comes to safeguarding data. We agreed that we could do still more to protect our own systems and the sensitive data entrusted to us by our clients. A true test of our systems required both penetration testing and social engineering — the "people and processes" portion of the security solution.

PENETRATION VS. SOCIAL ENGINEERING TESTS

To understand the difference between penetration testing and social engineering testing, compare your organization's network to your home.

Homeowners place locks and alarms on doors and windows to keep unwelcome parties from entering their residences. But not many homes have deadbolts on the interior doors because people trust their family and friends with unencumbered access inside their homes.

Network information systems are kept secure in much the same way; the perimeter is well guarded, but employees and other insiders can move about freely within the system, accessing the network's internal resources and data.

With such freedom comes the potential for problems. While many organizations strategize about the threats from outside their walls, your insiders – "your residents" – also constitute a security risk. Internal users can accidentally, negligently or intentionally expose your system to data breach from outside.

Awareness of both external (penetration) and internal (social engineering) vulnerabilities is critical to assess and improve your company's network security. During the security exercise, the company attempts to hack into a client's network from the outside to identify security weaknesses and flaws that could allow an actual attacker to compromise its systems. After identifying your system's vulnerabilities, the company recommends fixes.

Alternatively, social engineering testing is like testing and then training your family members to practice home safety – i.e., by not leaving doors unlocked or sharing sensitive information with strangers on the phone.

Social engineering is a nontechnical method of intrusion by hackers that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It's one of the greatest threats that organizations encounter today.

The most common approach is phishing attacks. In this case, the hacker, or phisher, sends an email that appears to come from a legitimate business

THE HUMAN FACTOR IN SECURITY

Nearly all social engineering techniques are based on specific attributes of human decision-making known as cognitive biases. These biases, sometimes called "bugs in the human hardware," are exploited in various combinations to create attack techniques to steal employees' confidential information.

Types of social engineering attacks can range from direct attacks – such as when data thieves phone employees and attempt to trick them into divulging their users IDs, passwords and other sensitive information – to indirect attacks – for example, posting a new help desk number on the company's lunchroom bulletin board.

However, the most common approach is phishing attacks. In this case, the hacker, or phisher, sends an email that appears to come from a legitimate business — a bank, or a credit card company — requesting "verification" of information and warning of dire consequence if it is not provided. The email usually contains a link to a fraudulent web page that looks legitimate, with company logos and content, and includes a form requesting such sensitive data as home addresses or PIN numbers.

Sometimes these fraudulent web pages will simply try to trick computers into attempting to perform network authentication. Using this approach, the fraudulent website can acquire user IDs and hashed passwords. A hashed password is an encrypted representation of the text people enter into the password field when they log in. On a network, this method of authentication allows legitimate users to move freely among network servers, databases and other resources without having to constantly relog in. There are many programs available to help hackers crack these hashed passwords.

SELECTING A SECURITY PARTNER

Data thieves grow more sophisticated in their techniques and attack strategies every day. That means organizations must also be proactive to get a true picture of their network vulnerabilities and risks. Seeing this shift, Wiss performed penetration and social engineering testing on our own network.

After several months of research, our company hired Grid32 to perform a full security test on our network, including both penetration testing and social engineering testing. Grid32 provides independent computer system and physical security audit services to organizations of all sizes, including the U.S. departments of Energy and Defense, Cisco and companies in the accounting industry.

The security test was performed without the knowledge of Wiss employees – ensuring our team members reacted normally to the threat scenarios. Here is a brief look at the results.

Penetration testing results. After several weeks of Grid32's intensive but unobtrusive testing, we were gratified to find that even the most intensive penetration testing had proved futile. Wiss' IT department had locked down the system in such a way that it was impervious to breach from the outside. Our social engineering test results yielded a different outcome, but one that would provide insightful feedback. Under several waves of carefully orchestrated social engineering attacks by our security partner, a handful of our internal employees had clicked suspicious email links leading to a fraudulent website set up by Grid32. At this point, it'd only be a matter of time before social engineers could crack passwords and gain unauthorized access into a company's network. From there, they could move through the network and resources as easily as trusted employees. Implementing these tests on our systems and educating our internal organization is just the start to preventing similar, real-life attacks on Wiss & Company.

Fully securing our network and our clients' data is now a core part of our internal culture.

THE WISS RESPONSE

Wiss undertook the holistic security testing approach not to embarrass anyone in our company but to be proactive and pinpoint our vulnerabilities. That knowledge is invaluable to any organization so that you can strengthen your people, process and technology to better protect against actual hackers.

While not sharing specific details of our security plans, we can address general approaches.

Ongoing employee education. Wiss now has a mandatory employee security awareness and education program. It will become part of our new hire orientation training and be used on an ongoing basis. Through constant and updated training, we're determined to strengthen our employee's security knowledge and ensure that they fully understand our internal security policies.

Password protection improvements. We will also be strengthening our password policy, requiring that passwords be more complex, longer and harder to crack, and mandating that passwords be changed frequently.

Technology upgrades. Wiss will continue to implement the latest intrusion prevention, detection and log monitoring technologies. These upgrades will allow our IT department to actively monitor and detect intruders to our perimeter defenses. Wiss has also changed its internal budgeting to include annual security penetration and social engineering testing to benchmark our progress and alert us to any new vulnerabilities.

CONCLUSION

Many employees see network security as the responsibility of IT staff and anti-virus software. At Wiss, we know that system security is everyone's business.

Fully securing our network and our clients' data is now a core part of our internal culture. We believe that every dollar we spend being proactive better protects our clients' sensitive information and is a far better approach than reacting to a breach that's already occurred.

Can you say the same? Let Wiss help you improve your network security.

For more information, contact Wiss at 973.994.9400.