www.pwc.com

Security for social networking

Advisory Services
Security

pwc

Threats to the corporate network have escalated as the use of social media has soared. It’s time to adopt a proactive strategy that reinforces effective user policies with robust technologies.

Table of contents

The heart of the matter

Social networking is pervasive in today's workplace. At any given moment, on-the-job employees are updating Facebook statuses, reading Twitter feeds, and networking on LinkedIn. Some may even be using social networking for legitimate business purposes.

Businesses have embraced social networking to strengthen collaboration and productivity by allowing easy access to the knowledge of co-workers. Outside of the workplace, social networking can help an organization attract and engage customers, improve the customer experience, and manage its brand image.

The use of social media for recruiting is becoming increasingly popular. Human resources departments have found that LinkedIn is essential to hiring skilled talent.

Trouble is, cyber criminals find social media equally useful.

Phishing, while certainly not new, is a common ploy used by intruders to obtain usernames and passwords, and eventually access the network, introduce malware, steal corporate information, and initiate other serious attacks. A phishing attack, which typically begins with an e-mail message, Facebook post, or tweet, exploits the user's trust by appearing to come from a friend or a company with which the user does business. Because social networking also is based on trust, phishing is an increasingly effective vector of attack on social media sites.

User credentials, when combined with data available on corporate websites, provide a rich resource of bait for phishing scams. Using LinkedIn, for instance, an attacker can discover a recruiter's connections within the company and spoof an e-message that appears to be from an HR co-worker. The intruder taps in a subject line that reads, "Take a look at this resume," then attaches a document bearing malware.

When the recruiter opens the e-mail and clicks the attached file, malware gains a beachhead on the enterprise network.

It is happening every day. A survey by the Ponemon Institute found that 52 percent of organizations have reported an increase in malware attacks over the past year due to employee use of social media in the workplace. [1]

Risks associated with social media are not limited to malware, however. Cyber criminals can mine networks to obtain valuable information from employees, steal intellectual property, highjack a website or social media account, and damage a company's reputation. Employees may unwittingly reveal proprietary corporate information or highly regulated data.

Clearly, social media is here to stay. Businesses can use it to great advantage, but they must first implement a proactive security strategy that creates effective user policies and reinforces them with technology that monitors and protects the enterprise.

[1] Ponemon Institute, Global Survey on Social Media Risks, September 2011

An in-depth discussion

There's no stopping social media. A recent Nielsen survey found that 80 percent of active Internet users spend time – a lot of time – on social networking sites. In fact, use of social media and blogs accounts for 23 percent of all time online, three times the amount of time spent using email (7.6%). [2]

Use of social media is not confined to off-hours, however. As Ponemon has noted, 60 percent of social media users of visit sites such as Facebook and Twitter for non-business purposes at least 30 minutes per day while at work. [3]

Of course, the use of social media in the workplace has its benefits. Organizations have embraced social media for tasks such as marketing, product design, and recruiting. Many have found that social media can increase productivity, spark innovation, and create a more collaborative corporate community.

Outside of the workplace, social networking can help a business reach and engage customers, improve the customer experience, help develop new products and services, and polish the brand image of the business. Many businesses today patrol sites such as Twitter and Facebook to listen in on the chatter about their products and services. Should the conversation turn negative, the company can use the same medium to respond and move the discussion in the right direction.

Consider Whole Foods, the grocery store chain that is the most-followed brand on Twitter and has an active Facebook presence, with more than 750,000 fans. The company's Twitter feed presents an engaging, friendly voice and sends out dozens of tweets to its 2 million followers daily, offering recipes, shopping specials, customer service, and more. Recently, a vegan follower reported that he had discovered a human fingernail in his Whole Foods vegan breakfast burrito. What could have been a public relations disaster was almost instantly defused by a quick Twitter exchange. The public conversation ended with the customer reporting that the store had delivered "great service very quickly."

Why social media may be hazardous to the corporate network

Before digital social networking, social-engineering culprits were called confidence or "con" men. They typically committed fraud through human interactions, a technique that was limited by the number of people they could reach.

Today's social engineers have gone digital. Phishing is an effective vector of attack, particularly when used in conjunction with social media, enables criminals to reach thousands of potential fraud victims. Targets of phishing attacks may unwittingly divulge usernames and passwords, credit card numbers, and other information that can be used for fraudulent purposes. In the workplace, phishing can lead to leakage of sensitive or regulated data, infect the network with malware, and provide an ingress for advanced persistent threat (APT), a tenacious criminal attempt to access information on an organization's computer systems.

[2] Nielsen, State of the Media: The Social Media Report – Q3 2011, September 2011

[3] Ponemon Institute, Global Survey on Social Media Risks, September 2011

As the use of social media rises, so do phishing expeditions: The Anti-Phishing Work Group reports that phishing attacks increased 58 percent during the first half of 2011 compared with the same period the year before. [4]

Adding to security concerns, phishing has become simplified and increasingly pervasive as traditional applications have been recast as mobile social media apps. Today, it is alarmingly commonplace for hackers to unleash malicious code on social media apps for smart phones. It is also very effective: Ponemon found that almost one in three (29%) security breaches result from malware borne by social media. [5]

Phishing, and the more targeted spear phishing, are also employed for sophisticated cyber crimes like APT. Threat. Recent APT attacks have employed phishing email messages that infect computers after users open a file or click a bogus link. Often, social media sites provide the employee information that enables intruders to craft an effective spear phishing email. This tactic, for instance, is believed to have been employed by the perpetrators of “Operation Aurora,” a coordinated cyber attack against Google and at least 30 other companies that was used to steal corporate intellectual property and gain access to user accounts.

Another danger, particularly for Twitter users, is the use of abbreviated URLs. URL shortening services from sites such as Bit.ly and is.gd obscure the destination of the link from the user, creating a particularly effective tool for cyber criminals. Indeed, Symantec reported that, during one three-month period, 65 percent of malicious URLs found on social networks were hiding behind shortened URLs. [6] A recent scam on Facebook, for instance, employed a shortened URL to lure users to a site to receive an iPad 2 for review. Not only did victims voluntarily surrender account information and personal data, they also infected their computers with malware.

Another way to uncover user account information is the use of data-mining scripts that “scrape” information from social networking sites. Many people use the same log-in information for multiple social media accounts, and this information is tempting and potentially profitable to criminals.

In late 2010, for instance, hackers compromised the servers of Gawker Media, a high-profile blog network, and obtained 1.4 million user passwords and other confidential information. The user information was posted on a public torrent, and within a matter of days spammers used the e-mail addresses and passwords lifted from Gawker’s servers to take control of Twitter accounts.

Not all information leaks result from the efforts of criminals, however. Employees themselves may voluntarily disclose critical business information and intellectual property. As we have seen, many users post to social media sites from work, and they can inadvertently disclose sensitive business information such as confidential details about a software project or a new product under development. Use of location-based social networking apps also can unintentionally provide information that can be exploited by competitors. For instance, an employee who broadcasts his or her whereabouts by “checking in” to locations using Foursquare might compromise an acquisition if the employee repeatedly checks into the target company’s location during negotiations

In addition to personal and business information, data leakage also can violate confidentiality mandates. For instance, we have seen numerous cases in which a

[4] Anti-Phishing Work Group, Global Phishing Survey: Trends and Domain Name Use in 1H2011, November 2011

[5] Ponemon Institute, Perceptions About Network Security, June 2011

[6] Symantec, Symantec Internet Security Threat Report: Trends for 2010, April 2011

healthcare employee posted information about a patient's medical records on social media, a clear violation of the Health Insurance Portability and Accountability Act. The practice may be more common than you think: A study by Websense found that 20 percent of IT managers reported they had seen confidential information posted on social networking sites.[7]

How businesses can balance security and social networking

To reap the benefits of social media – and avoid the potential threats – businesses should embrace social networking and implement a proactive strategy to safeguard corporate networks and data. It is critical that the security strategy be backed by rigorous – and continuous – employee awareness and training.

We believe a social media strategy should be two-pronged: It should set forth policies and procedures that govern the use of social networks and corporate information, and it must back up those policies with technology that protects the safety and integrity of data and the corporate network.

An effective approach requires that the business and technology sides of the company are united and fully committed to a social networking security strategy. The two must analyze content and policies in detail, as well as determine the right mix of enterprise technologies to monitor, classify, and manage data.

The first step will be to form a business strategy that articulates and communicates how the organization intends to leverage social media and includes a long-term adoption plan for policies, procedures, and solutions. At the onset, stakeholders must plan customized awareness and training programs for employees.

It is essential that the business classify data so that employees understand precisely what is – and is not – sensitive information. This process should specifically delineate how employees may use sensitive data, as well as define who is authorized to access and share corporate content.

Policy also must clarify the types of social networking accounts the company sponsors. For instance, the business should ensure that employees understand the difference between a company-sponsored Twitter or Facebook account and individual company accounts run by a person or team. Everyone must know that these corporate accounts are very different from an employee's personal account.

What's more, the business must clearly specify who is responsible for particular types of communications using social media; these operational roles typically fall within the marketing and customer service departments. The company also should establish management oversight for social media, designating both a chief strategist and a community manager, for instance.

Businesses must be specific about what information can be posted to specific social networking sites. For instance, employees may be permitted to include employer affiliation on a public profile on LinkedIn but not on Facebook; policies may vary by role. HR specialists, for instance, may be permitted to provide more company information on sites such as LinkedIn because doing so is essential to recruiting efforts.

[7] Websense, Security Pros & "Cons," October 2011

Policy also should specify whether employees may access social networking sites from corporate-owned devices such as smart phones and tablets, and which apps may be used to access social media. Enforcement mechanisms will be required to ensure that policies are followed.

When developing roles and policies, the business should include a strategy for employee separation to maintain ownership of intellectual property and social identities. For example, if an employee is assigned to monitor Twitter feeds for customer service complaints and opportunities, he or she must understand that the company owns this online identity and that it must be relinquished upon termination or voluntary separation.

No strategy is complete without a remediation plan. The business should plan how it will manage reputational damage and respond to critical online commentary. Social networking can instantly create buzz as well a blizzard of negative publicity, so the strategy should include a game plan to quickly evaluate the situation and act appropriately and swiftly.

Establishing social media policies is only the beginning: The real work lies in getting employees to make behavioural changes. The success of any social networking security program will hinge upon thorough and continuous education of the workforce.

Design of an awareness and training program should begin at the earliest phase of strategy discussions. It is critical that the business understands the current security knowledge of its workers and tailor education to these specific knowledge levels. To ensure success, it will be essential to obtain buy-in from senior management and ensure that business unit managers reinforce the importance of training. Of course, Human Resources also should also be involved in developing the security-learning program.

Security training should be engaging, targeted, and interactive. A “learn by doing” approach presented in short sessions that include peer interaction will boost retention of knowledge. Effective education might include, for instance, scenario-based training that describes up-to-date scams employed by social media attackers or how to identify a phishing website. Emphasize that this knowledge will be as useful at home as it is in the workplace.

Customized training sessions should demonstrate how current threats originate on social media and how they can be downloaded to an individual computer or mobile device and then infiltrate the enterprise network. The business risks of malware, data loss, APT, and other threats should be described in very real and convincing scenarios that are applicable to the individual business.

It is important to note that education should not be exclusively technical. In today’s digital-social world, sharing information via social media has become so reflexive that many employees may not realize that data innocently posted on a social network can harm a business. They also must understand that if, at any time, they identify themselves as an employee of the business, they are representing the company to the digital world. Anything they say online about the company becomes part of the public discussion and can have a potentially harmful impact on the business.

Finally, it is critical that businesses fully detail the consequences - both the company and the individual – of noncompliance with social media policies. Policies should state that employee use of social media might violate the corporate code of conduct for privacy, client confidentiality and intellectual property. Be clear: Jobs are at risk.

Why technology is essential to an effective security strategy

Strong policies and awareness programs can be reinforced with appropriate technology enforcement and monitoring solutions that protect against malware, data leakage, and other suspicious activity.

Possible strategies include multilayered security at the gateway and the end points, content classification, content filtering, data loss prevention (DLP), and mobile device management (MDM) solutions. Identifying the right combination of these security tools can be a daunting challenge because Web 2.0 technology is freewheeling and constantly evolving.

Effective security for social networking must leverage both decentralized and centralized modes of IT security. In other words, the business must protect both the network and the end points.

Start with centralized security, which holds the key to safeguarding the enterprise's data and network resources. As hackers become more aggressive in attacks using social media, businesses must continue to step up the use of traditional protection tools such as scanning to verify incoming traffic and configuring their Internet gateway to block malicious exploits such as cross-site scripting and phishing. Another option is inbound content filtering, which employs spam blockers and anti-virus applications to block or allow a communication based on analysis of its content.

For outgoing traffic, a DLP solution enables the business to screen content before it leaves the corporate network. It monitors outbound traffic to detect and potentially stop the communication of sensitive information. DLP can identify sensitive data at rest, control its use at end points, and monitor or block its egress from network perimeters. In practical terms, that means DLP can quarantine an unauthorized or underprotected message that contains unencrypted personal information before it leaves the network.

At the end points, businesses should lock down users' Web browsers to block JavaScript and plug-in capabilities – a critical step because many social media sites push much of the application logic to the Web browser. JavaScript and plug-ins deliver much better end-user experiences, but they may also introduce additional vulnerabilities that open the network and data to attack.

Finally, remember that mobile devices such as smart-phones have become the new frontier for hackers. Every social media security policy must protect the integrity of the device and the sensitive data stored on it. New mobile device management tools automate cross-platform management of handhelds with a common set of policies and help safeguard corporate data by filtering activity based on management security policies. An MDM client is installed on mobile devices and enables capabilities such as remote wipe and lock, device encryption, and password enforcement.

Risks also exist outside the enterprise, and many businesses will want to protect their brands and strengthen customer service and marketing initiatives by actively monitoring social-digital conversations. Every day, more than 250 million tweets are posted on Twitter alone; obviously, no company can monitor the entirety of social discussions.

The business must decide what media should be monitored and revisit that policy periodically. It is important to note that, in some cases, risks could escalate into legal issues; counsel, therefore, should have input into monitoring strategies.

There is no shortage of monitoring tools and services to help businesses protect their brand and reputation. Most businesses prefer monitoring services that track and assess mention of a company in blogs, forums, social networks, and video- and photo-sharing sites, then aggregate results into positive and negative categories for quick review.

What this means for your business

As risks associated with social networking escalate, businesses must take extraordinary care to craft an integrated security strategy that balances employee education with sophisticated network monitoring and data protection technology. This initiative will require a united partnership between the business and information technology groups.

PwC believes businesses must approach social networking with equal measures of opportunity, caution, and careful planning. The activities, risks, and technologies associated with social networking are constantly evolving as the types of social media sites and applications proliferate. It is essential that the business develop a life-cycle strategy that can address current needs and quickly adapt to changes in the social networking landscape.

Effective security for social networking requires that organizations fuse education and behavioral change of employees with robust technology that constantly monitors for risks. This approach demands experience in behavioral change, as well as deep knowledge of data classification, Web applications, network monitoring, and enterprise security.

As social media proliferates and gains more users, it is essential that a strategy and solution be implemented by professionals with expertise in the current state of social networking risks. PwC is a recognized, trusted leader in security consulting with global experience in the scope of solutions for data protection, data classification, and compliance. Our team assesses security and privacy risks and helps to implement solutions to mitigate these risks.

Social networking, at its essence, is more about following knowledge than people. We believe, however, that effective security requires that businesses lead – not follow –with a knowledgeable strategy to protect enterprise resources. We can help.

Contacts

To have a deeper conversation on the industry or on any of the topics mentioned, please contact:

Gary Loveland
Principal, National Security Leader
gary.loveland@us.pwc.com

Brad Bauch
Principal, Houston
brad.bauch@us.pwc.com

Rik Boren
Partner, St. Louis
rik.boren@us.pwc.com

Kevin Campbell
Partner, Atlanta
kevin.campbell@us.pwc.com

Michael Compton
Principal, Detroit
michael.d.compton@us.pwc.com

Shawn Connors
Principal, New York
shawn.joseph.connors@us.pwc.com

Scott Evoy
Principal, Boston
scott.evoy@us.pwc.com

Joe Greene
Principal, Minneapolis
joe.greene@us.pwc.com

Peter Harries
Principal, Phoenix
peter.harries@us.pwc.com

John Hunt
Principal, Washington
john.d.hunt@us.pwc.com

Jerry Lewis
Principal, Dallas
jerry.w.lewis@us.pwc.com

Mark Lobel
Principal, New York
mark.a.lobel@us.pwc.com

Sloane Menkes
Principal, Washington
sloane.menkes@us.pwc.com

Joe Nocera
Principal, Chicago
joseph.nocera@us.pwc.com

Chris O'Hara
Principal, San Jose
christopher.ohara@us.pwc.com

Fred Rica
Principal, New York
frederick.j.rica@us.pwc.com

Sohail Siddiqi
Principal, San Jose
sohail.siddiqi@us.pwc.com

Andy Toner
Principal, New York
andrew.toner@us.pwc.com

pwc.com

This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

The information contained in this document is provided "as is," for general guidance on matters of interest only. PricewaterhouseCoopers is not herein engaged in rendering legal, accounting, tax, or other professional advice and services. Before making any decision or taking any action, you should consult a competent professional adviser.