Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Reducing the Risks of Social Media to Your Organization

Social media offers important business advantages to companies and organizations, but also has well-known security risks. In order to mitigate these security risks and still enjoy the benefits of social media organizations must establish and enforce good social media usage policies. But many organizations are unsure of how to develop effective social media policies. Instead, many organizations either simply prohibit social media use altogether, or have no policy at all regarding social media use. Both of these approach...

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.
watchfire

Security Policy and Social Media Use

GIAC (GSEC) Gold Certification

Author: Maxwell Chi, maxwell.chi@sbcglobal.net
Advisor: Rick Wanner

Accepted: March 16, 2011

Abstract

Social media offers important business advantages to companies and organizations, but also has well-known security risks. In order to mitigate these security risks and still enjoy the benefits of social media organizations must establish and enforce good social media usage policies. But many organizations are unsure of how to develop effective social media policies. Instead, many organizations either simply prohibit social media use altogether, or have no policy at all regarding social media use. Both of these approaches are unsatisfactory. Organizations that do not adopt social media fail to reap its significant benefits and are at a disadvantage to their competitors that do. Organizations that simply allow social media use without any policies or guidelines open themselves to security threats. This paper is intended to demonstrate that the existing information security policies already in place at many organizations can easily be extended to cover social media. Therefore, organizations do not need to issue security policies and guidelines specifically for social media. The paper attempts to demonstrate that the main security threats posed by social media would be addressed by a good overall security awareness program, along with and technical and administrative safeguards.

© 2011 SANS Institute, Author retains full rights.

1. Introduction

Social media is "the internet and mobile technology based channels of communication in which people share content with each other. Examples are social networking sites such as Facebook and Twitter." (Financial Times Lexicon, 2011). Social media can offer business advantages for both private companies and government agencies. Organizations can use this media to reach out to mass audiences efficiently and at very low cost. They can promote brand awareness in many different markets. They can also network with current and potential customers.

A dichotomy exists between companies that have embraced the promise of this new technology and those that mostly avoid it. In a 2009 survey of companies that participate in online social media communities, 70 percent of respondents reported using social media of some kind in their businesses (Gordon, n.d.). Over 40 percent of such companies had employees whose job function included spending time on social media sites in order to maintain an organizational presence. More than a quarter of these companies maintained social media sites for employees' personal announcements and social events. Fewer than ten percent blocked access to social media for any employees.

A 2009 survey of companies, however, found that 54 percent of respondents banned the use of social media while at work, while 20 percent allowed use of social media only for business purposes (Gaudin,, 2009).

Social media can have tremendous benefits but also can have serious security risks for organizations. Two of the greatest risks to organizations are malware and inadvertent disclosure of sensitive information (Waxer, 2011). The security risks are often cited by companies as a reason they do not allow social media use. Seventy-two percent of companies believe employees' use of social media poses a threat to their organizations (Schroeder, 2010). Their concerns are justified. According to a report by Sophos, the incidence of malware is increasing on the most popular social media sites including Twitter, MySpace, Facebook and LinkedIn (Sophos, 2010). In 2010, 57% of users reported they received spam via social media sites, an increase of 70.6% compared to the previous year. Additionally, 36% of users report they were sent malware via social media sites, a rise of 69.8% over 2009 (Schroeder, 2010).

Maxwell Chi, maxwell.chi@sbcglobal.net

© 2011 SANS Institute, Author retains full rights.

Businesses, including small and medium-sized businesses (SMBs), have also been victims of Internet attacks. In a 2009 survey, 24% of SMBs reported having been compromised by employees who used social media sites; 25% by employees who used peer-to-peer networking sites; and 32% by workers who downloaded media (Webroot, 2010). Even companies that strongly believed they devoted sufficient resources to information security reported successful attacks from viruses (60% of respondents), spyware (57%), and phishing (47%). Security breaches against SMBs are particularly troublesome because many of them lack the resources to adequately contain and recover from attacks.

As with all information technologies, organizations must understand the security threats associated with social media and must establish and enforce good policies in order to mitigate the security threats. But corporate policies have largely not kept up with the rapid adoption of social media. Of the companies that actively participate in social media, fewer than 25 percent have official policies regarding blogging. Over 40 percent have no specific corporate policies regarding use of social media (Gordon, n.d.).

This paper is intended to make a case that many organizations actually do not need to issue new end-user security policies and guidelines specifically for social media. This is because the main threats posed by social media use related to end-user behavior would be addressed by most organizations' existing security awareness programs. Phishing, social engineering, viruses, and misuse of resources are already covered in recommended security policies and awareness training for most organizations. The contention is that a good overall information security policy, combined with training, enforcement, and proper security safeguards, can help mitigate the main threats to organizations posed by employees' use of social media.

The thesis of this paper is that the main security threats to an organization from social media would be addressed by a general information security policy, and therefore most organizations do not need a security policy specific for social media. The following sections develop the thesis of the paper. Section two provides background on the business benefits of social media and reasons why some organizations are hesitant to adopt it. Section three describes the main security threats to the organization from social media. Section four summarizes the relevant components of a recommended organizational

Maxwell Chi, maxwell.chi@sbcglobal.net

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

security policy. Section five shows how the provisions of this policy would mitigate the major social media threats. Finally, section six summarizes issues related to enforcement of security policies and describes some emerging security technologies that can help organizations with enforcement.

2. Background

Social media sites like Facebook, Twitter, and LinkedIn have dramatically transformed the way people interact with others on a global scale. They also have reshaped the way many companies promote their brands, advertise and distribute their products and services, and network with customers. In order to reach and connect with an increasingly digital marketplace, many companies are realizing they must maintain an active presence in the social media world, since that is where many of their customers are. According to surveys, nearly 60 percent of Internet users in the U.S., or 127 million people, use a social media site at least once a month, and many use one far more often than that. By 2014, projections are that two-thirds of all U.S. Internet users will use a social media site at least occasionally. ComScore, Inc. has reported that Facebook is currently the fourth most-visited website, behind search engines Yahoo!, Google and Microsoft (Rubin, 2010a).

Companies that incorporate social media into their business practices are reporting significant benefits. In a survey by McKinsey & Company of executives from around the world (McKinsey, 2009), 69 percent reported that their companies had gained measurable business benefits, including improved products, services, and marketing, lower cost of doing business, and higher revenues. The more use a company made of social media, the greater the benefits tended to be. The companies that derived the most benefits did so not only by incorporating social media technologies with the work flows of their employees, but also by closely linking themselves with customers and suppliers using the technologies. Despite the current economic environment, respondents overwhelmingly said that they would continue to invest in social media technology. Another study found that seven out of 10 consumers are more likely to use a local business if it has information available on a social media site (Rubin, 2010b).

Maxwell Chi, maxwell.chi@sbcglobal.net

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Some companies are intrigued by the business case for social media. Surveys by various consulting firms find that company executives are increasingly receptive to social media and online collaboration tools (Fraser and Dutta, 2009). Forrester projects overall spending on these tools to grow at 43 percent annually, from $764 million in 2008 to $4.6 billion in 2013.

In many other organizations, however, there is still wariness about social media. The $4.6 billion projected to be spent on social media would still represent less than one percent of global corporate spending on enterprise software. Some companies are concerned about lost productivity caused by employees viewing Facebook or YouTube at the workplace instead of working. Companies all over the world put up with 45% of their employees' productive time being wasted on these and similar sites (Satyanarayana, 2009). Others point to the threats of social media such as malware, illegal activities, and damage to company reputation. Additionally, there are risks to corporate data security (Fraser and Dutta, 2009).

These concerns have led many companies to ban social media sites outright. Credit Suisse, Dresdner Kleinwort, British Gas, and Lloyds TSB use security systems to block access to social media sites. Citigroup, Goldman Sachs, JPMorgan and UBS restrict access to Facebook.

But adoption of social media in the corporate sector is gaining momentum as some of the world's most powerful technology companies including Intel, IBM, Cisco, and Google have embraced social media technologies. Also, as younger generations of employees enter the workforce, they will be expecting employers to use these technologies in the office (Gaudin, 2007). As more organizations continue to jump on to social media, soon a critical mass will be reached, and the remaining companies will be forced to adopt this technology in order to remain competitive. It is therefore important for companies to begin addressing their security-related concerns with social media.

3. Threats to Organizations from Social Media

In 2009, the Secure Enterprise 2.0 Forum issued its annual industry report which focused on social media security threats (Perez, 2009). The Secure Enterprise 2.0 Forum consists of executives at Fortune 500 companies which have adopted social media tools

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

and services in their businesses. The forum promotes awareness, industry standards, best practices, and interoperability issues related to the use of the new tools in the workplace. The report was intended to help companies that were considering adopting social media tools in their businesses by providing a basis for assessing the security risks. The report described the types of threats that social media technologies could pose in a business environment. The eight main threats identified in the report were:

3.1. Insufficient Authentication Controls

In many social media applications, sensitive information is spread among many different locations. This makes it more likely that an inexperienced user will introduce a weakness that will adversely affect the entire system. For example, there might be some administrative accounts for which the correct security controls are not in place, such as sufficiently strong passwords. An attacker could use a brute-force attack to determine the password of one account; if other accounts are connected to it through a single-sign-on arrangement, the attacker would then have administrative access to a number of systems.

3.2. Cross Site Scripting (XSS)

Cross site scripting is a type of attack in which the victim's web browser is induced to execute malicious code. Depending on the type of attack, the malicious code may steal the victim's personal information, enabling the attacker to impersonate the victim, or cause the victim's computer to launch an attack against a third party without either the victim's or the third party's knowledge (Timm and Perez, 2010).

3.3. Cross Site Request Forgery (CSRF)

Cross site request forgery is an attack which causes an end user's web browser to execute actions of the attacker's choosing without the user's knowledge. By embedding a malicious link in a web page or sending a link via email or chat, an attacker may cause the users of a web application to perform unwanted actions. More specifically, the attacker causes the user's browser to make requests to a web site to which it has been authenticated, without the user's or the web site's knowledge. These actions may result in compromised end user data and operations, or even an entire server or network.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

There are various types of CSRF attacks. Below is an example of an attack scenario (Schroder, 2009).

Step 1: A user logs in to a web site using their login credentials.

Step 2: The site provides the user with a cookie to use to identify the user to the web site for the current session. The cookie is stored in the browser.

Step 3: The user finishes their business on the site, and then views another site while still logged in at the first site.

Step 4: Unknown to the user, the second site contains a malicious script. The script could be hidden or disguised as an image. Nevertheless, the user's browser will execute the script.

Step 5: The malicious script causes the user's browser to return to the first site and use the user's credentials to perform some unwanted action. This action might be to change data on the user's account, or reset the user's password and email it to an address accessible to the attacker. The point is that the user did not request or desire this action to be performed, and to the first web site, it appears that the user is performing it, whereas it was really the user's browser under the attacker's control.

There are two main types of CSRF attacks: stored, or persistent, and reflected, or nonpersistent. In a stored CSRF attack, the attacker can use an application to provide the user with the exploit link or other code. This code sends the user's browser back into the application, and causes attacker controlled actions to be executed as the victim. In a reflected CSRF vulnerability the attacker sends the link to the user outside of the application. This may be an email message, an instant message, a message board posting, or even a flyer in a public place with a URL that a victim types in (Burns, 2007). Stored CSRF vulnerabilities are more likely to succeed, since at the time the user receives the exploit content they are more likely to be authenticated to the site and able to perform the actions desired by the attacker. However, stored CSRF attacks also leave a trail, which may lead back to the attacker. Reflected CSRF attacks are less likely to succeed, as the user may not be logged into the web site when the exploits are tried. Also, the trail from a reflected CSRF attack may be under the control of the attacker, however, and it is easier for the attacker to cover their tracks.

Maxwell Chi, maxwell.chi@sbcglobal.net

© 2011 SANS Institute, Author retains full rights.

CSRF attacks are not unique to social media: these types of attacks have been known since the early 2000s, and conventional web sites are also susceptible to CSRF attacks (Zeller, 2008). For example, a vulnerability, which has been fixed, was found on ING's website (ingdirect.com) that allowed additional accounts to be created on behalf of a user. This vulnerability also enabled an attacker to transfer funds out of users' bank accounts. A vulnerability also was found on Metafilter that allowed an attacker to take control of a user's account, set a user's email address to the attacker's address, and send the user's password to the attacker's email address.

However, the features of some social media sites make them particularly vulnerable to CSRF attacks. In 2009, a CSRF vulnerability, which has since been fixed, was discovered in Facebook (Timm & Perez, 2010). The vulnerability existed in the Facebook Application API. It enabled an attacker to create a Facebook application that forwarded a user's personal information to the attacker's application server without either the user's or Facebook's knowledge. The vulnerability was based on the fact that Facebook routed requests from a user's browser and responses from applications through the Facebook platform. In this case, an attacker would have been able to embed malicious code in a third-party web page. When the user's browser requested to download the web page, the code would have redirected the request through the Facebook platform and sent it, along with the user's personal information, to the attacker's application server. From there, the request would have been redirected to the correct web server. Neither the user nor Facebook would have had any knowledge that the attack had occurred.

3.4. Phishing

Although phishing is not unique to social media, there has been a recent spike in phishing attacks associated with social media sites (Fisher, 2011). Many people view social media sites on cell phones or other mobile devices. This makes it harder to distinguish real and fake web sites. Additionally, social media enables attackers to send phishing messages that appear to come from someone that the victim knows. Having obtained login information for a few accounts, scammers will then send out messages to everyone connected to the compromised accounts, often with an enticing subject line that suggests familiarity with the victims (Baker, 2009).

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

3.5. Information Leakage

With the advent of "always-on" connectivity, the traditional lines between work and personal life are becoming blurred. Particularly, younger workers use the same technologies in the office as at home. Additionally, social media sites like Facebook and Twitter create the illusion of familiarity and intimacy on the Internet. The result is that people may be inclined to share information on the Internet that their employer would have preferred to keep private. Individuals may not be divulging trade secrets, but the cumulative effect of small, seemingly innocuous details can enable a business's competitors to gain valuable intelligence about that company's business situation and future plans.

3.6. Injection Flaws

The technologies that social media uses make it vulnerable to injection attacks such as XML injection. Additionally, social media applications often rely on client side code, so they rely heavily on client-side input validation which an attacker can bypass.

3.7. Information Integrity

Data integrity is one of the foundations of information security. Malware introduced on a platform or network can modify user information and databases. Users who do not diligently update their antivirus software can make their systems vulnerable. An attacker could deliberately modify data in transit or storage through malware or direct manipulation, but legitimate users also make honest mistakes. Unintentional misinformation is frequently posted on the Internet, which is then taken as fact by many viewers. In social media, data is stored in many places where many different users can access it. Having data accessible to many users increases the chance that a malicious or mistaken user could post inaccurate information, which compromises data integrity.

3.8. Insufficient Anti-automation

The interfaces of social media applications are susceptible to automated attacks, such as automated running of queries, automated retrieval of large amounts of

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

information, and the automated opening of accounts. Anti-automation mechanisms like CAPTCHAs can help defeat or at least hinder these types of attacks.

In examining the preceding list of social media threats, one sees that the main threats to social media are largely the same as those to traditional web applications. Cross-site scripting, phishing, and inadvertent data modification and information leakage are not new threats, nor are they unique to social media. But the nature of social media technologies can often increase their vulnerability to these threats. In 2009, the U.S. military considered a near-total ban on social media sites throughout the Department of Defense. Military officials cited inherent technical security weaknesses and lack of security safeguards on social media sites (Schachtman, 2009).

The threats described previously can be broadly classified into two categories: those related to end user behavior (insufficient authentication controls, phishing, information leakage, and information integrity), and those that are related to security vulnerabilities within the application (XSS, CSRF, injection flaws, and insufficient anti-automation). A combination of proper end-user security along with secure coding practices and verifications should therefore help mitigate both sets of risks.

The next section summarizes the relevant components of a recommended end-user security policy. This provides the basis for section five, which shows how a general end-user security policy would address the main threats from social media.

4. Components of a End-User Security Program

This section summarizes the components of a recommended end-user information security program that are directly relevant to social media security. Brodie (2009) and the SANS suggested Acceptable Use Policy (2006) give outlines of a general end-user security program and what topics should be covered. The pertinent parts are summarized below.

4.1. Desktop Security

The focus of the desktop security section is to educate users why it is important to use a password-protected screen saver and to lock their computers when the users walk away from them. The computers should also have a screensaver timeout so if the user

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

leaves their computer, the password-protected screensaver comes up after a short time. Again, the idea is to keep out both insiders and outside attackers. If a potential attacker has access to a user's computer that is left unguarded, they could install malware or steal sensitive data. Users should also be wary of shoulder surfing.

4.2. Password Security

The password security section should set forth the minimum password requirements of the organization and emphasize selection of strong passwords. Additionally, password security is a crucial concern. Sharing passwords as well as leaving them out where others could discover them should be strongly discouraged.

4.3. Phishing

Phishing attacks are very common and, unfortunately, often very effective. Security awareness training should provide examples of phishing attacks and emphasize proper precautions (e.g. disregard and delete suspicious electronic messages and avoid clicking on links provided in e-mail and other communications). Brodie suggests having users take a phishing IQ test, and having security administrators report phishing attempts to phishing web sites such as PhishTank and The Anti-Abuse Project.

4.4. Malware

Brodie recommends that the different malware categories such as viruses, worms, Trojans, spyware, and adware should be defined and then safeguards explained for each. The training in this area should emphasize prevention, identification, containment, and eradication of malware and a malware infection. For example, employees should ensure up-to-date antivirus and antispyware software are installed on all computers they use and understand the importance of performing regular scans not only of their computers, but also of any file they download from a web site, e-mail, or flash drive.

4.5. Internet Privacy

A major concern to many organizations is sharing of confidential or sensitive information by officers or employees on the Internet. The SANS Institute's suggested

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Acceptable Use Policy for computer end-users states that "Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>'s Confidential Information policy when engaged in blogging." (SANS, 2006, p. 4).

5. Organization Security Policy Mitigates Social Media Security Threats

The preceding section summarized the relevant components of a recommended organizational security policy. This section describes how such a policy can address the major social media security threats listed in section three. The first parts of this section will show how the security policy would mitigate threats related to end-user behavior. The last part of the section will describe how the security policy can help mitigate threats related to the web application itself.

In section three, four threats were listed that were related to end-user behavior. These are insufficient authentication controls, phishing, information leakage, and information integrity. The following parts of this section will describe how various components of an end-user information security awareness program could help mitigate these threats. Each information security component will be described along with the threat or threats that component would help mitigate.

5.1. Password Security Mitigates Insufficient Authentication Controls

The threat from insufficient authentication controls could be mitigated by the password security portion of an organizational security policy. In many social media applications, data is distributed in various locations. Some of these are under the control of relatively inexperienced users. According to a global survey, 44 percent of workers share devices with others without supervision, and 18 percent share passwords with colleagues (Cisco, 2008b). If an attacker were able to gain access to a database, server, or network by exploiting a user's account with insufficient authentication controls, the attacker could steal or modify sensitive data, or launch other attacks against the company's information resources. If the user had used the same authentication controls on other accounts, the attacker would now have immediate access to a variety of platforms or applications.

Maxwell Chi, maxwell.chi@sbcglobal.net

© 2011 SANS Institute, Author retains full rights.

Password security would help offset these risks. As stated in section 4.2, password security is a crucial part of a recommended security policy. Good password security would make it much harder for an attacker to gain access to a protected account or database.

Part of recommended password security policy is maintaining a different password for each account (SANS, n.d.). Many users have a large number of web sites and software applications that they use regularly; for simplicity, it is natural to want to use the same password on all or most of these. This behavior should be discouraged, as it exposes the entire suite of applications to an attacker who is successful at obtaining the password. Users should be encouraged to use different passwords on different sites.

Another important aspect of password policy is using strong passwords (SANS, n.d.). Users should be taught to choose strong passwords that they can memorize without having to write them down on a sheet of paper near their computer, where they could be exposed. In a study by Acunetix, 42 percent of Hotmail accounts had poor passwords (Timm and Perez, 2010).

There are well-known techniques for creating strong, yet memorizable passwords. For example, Byte Interactive's Good Passwords web site (http://www.goodpassword.com) assists in generating strong passwords, up to 60 characters in length, that are aligned with the keys on a standard keyboard to assist in recall. Another application is Password Safe, available from http://sourceforge.net/projects/passwordsafe/, which enables a user to maintain an encrypted database of passwords on their computer or to generate secure passwords on request. To aid in memorization, users might also consider grouping passwords by category of site or application. For example, a strong core password might be reused but with variations in beginning or ending characters. Passwords for financial sites might begin with F, while school sites might use the same core password, preceded by an initial string of characters that start with S.

The practice of using strong passwords should be encouraged and enforced through systematic checks. For company software applications, networks, and web sites, an automated password verifier should be used to verify the strength of a password chosen by each user at the time the user chooses it. Furthermore, automated password

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

checkers are available to test the strength of passwords used on networks and software applications.

Users should also be encouraged to change their passwords regularly. A reasonable length of time should be set after which users are required to change their passwords. Use of encrypted password databases on users' desktops may help lessen the resistance and difficulty associated with periodic password changes.

5.2. Safe Message Handling Mitigates Phishing, XSS, And CSRF Threats

In a security program like the one described in section three, users are strongly advised not to respond to suspicious messages and not to click on links within messages. Such a policy would mitigate the danger from phishing, XSS, and CSRF. Although these threats are not unique to social media, social media sites are often the platform of choice for attackers to launch such attacks. Twitter, Facebook, and MySpace have all been used to create or facilitate phishing attacks (Timm & Perez, 2010). A good security program, such as the one outlined previously, directly addresses phishing and how users can protect themselves. Because social media tend to create a false sense of intimacy on the Internet, users should be especially wary of phishing attacks. In social media sites, users are often quick to accept messages purporting to be from friends or acquaintances at face value without validation. Such messages often have enticing subject lines or contents, leading users to perform actions desired by the attacker, such as opening attachments or running applications.

In social media, users should be particularly circumspect when they receive a message from a friend or acquaintance that asks them to take some action. Before taking any action, they should consider the message and its contents, and think whether the friend or acquaintance is likely to send a message of this type. They should look at the writing style and consider whether it is similar to that person's writing style. They should also consider whether this message is similar to previous messages they have received from that person.

If the message appears suspicious, the user should disregard it, even if the return address and links appear authentic. A link could send the user initially to Facebook, for example, but then redirect to another site. The sender's computer may have been

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

compromised by an attacker and have sent the message without the sender's knowledge. If the user has doubts about the authenticity of a message, the easiest, and most prudent, thing to do may be simply to contact the sender by phone or in person and verify the message's authenticity. If the sender is a company, the user could contact the company's service agents or other representatives. Additionally, there are many antiphishing verification sites and products available, such as those from Comodo (http://www.vengine.com).

Proper caution regarding electronic messages is also recommended security policy, as described in section 4.3. This is an end user behavior that can help prevent XSS and CSRF attacks. Users should be encouraged not to click on links in emails, particularly if they do not recognize or trust the email or its sender. They also should not click on links within web sites unless they are sure it is safe to do so. Users should especially avoid clicking on links that point to secure web sites, such as banking sites. When accessing a web site, users should go to that site directly and not access it through a third-party site, which may contain a XSS vulnerability. All of these are recommended practices in a good security program.

5.3. Anti-Malware Software Mitigates Phishing, Information Integrity Threats

As stated in section 4.4, any information security program should emphasize keeping up to date with operating system patches and antivirus and antispyware software. In many organizations this is done routinely by system or network administrators without end user involvement. Anti-malware software would help address the risks from phishing and information integrity. Updated anti-malware software would mitigate the damage that could be caused by viruses or spyware that might be introduced from a phishing attack. It is also to prevent the user's machine from being compromised and used as a launching point for future attacks.

Anti-malware software would also address threats to information integrity. In social media, data is stored in various locations and controlled by users with varying levels of experience. Critical data can be inadvertently modified directly by an attacker, by malware introduced into a server or network, or accidentally by a user. To help protect against malware, users should ensure their antivirus software is up to date. Firewalls,

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

intrusion prevention systems, and application gateways are good ways to protect networks from outside attack. Proper user education and training and data cross-checking can help prevent accidental data modification.

5.4. Privacy Policies Mitigate Information Leakage Threat

A constant concern for companies is their employees disclosing information that the companies would prefer to remain secret. Even small, seemingly harmless details, put together, could enable competitors could gain valuable business intelligence about a company. The nature of social media is sometimes conducive to people revealing more information than they should. First, social media creates a false sense of familiarity and intimacy. Many people have long-term online relationships with others whom they met on social media sites, even though they do not really know much about the other people. Such long-term familiarity can lead many people to let their guard down and disclose more than they otherwise would. Second, in order to cultivate a following online and gain more friendships, some people may be inclined to reveal interesting pieces of information to which they are privy. In doing so, people may inadvertently cross the line into unveiling sensitive information.

Even those who are accustomed to handling and protecting sensitive information can easily fall into this trap. In 2009, the wife of Sir John Sawers, incoming head of the British intelligence agency MI6, posted family details on her Facebook account (Evans, 2009). These included the location of the couple's home and of their three children and Sawers's parents. This information was available to all of Facebook's users, as there was no privacy protection on the account.

Estimates are that 70 to 80 percent of security breaches are caused by insiders (Hirschhorn, 2007). Some of these are malicious acts by employees to steal sensitive data for profit or personal gain. But more frequent are genuine mistakes by well-intentioned workers whose actions result in data loss. Misplaced and stolen laptops, careless emailing of sensitive data, and inadvertent posting of documents on an internet site are common ways that information is lost in organizations. In 2009, the U.S. Department of Veterans Affairs settled for $20 million a class action lawsuit filed on behalf of 26 million current

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

and former military members whose sensitive personal data were on a single laptop stolen during a burglary in 2006 (Frieden, 2009).

Proper protection of sensitive data on the Internet is an important part of end-user security policy and was listed in section 4.5. Proper end-user information security training and due care can help prevent data breaches. Additionally, more organizations are relying on data loss prevention measures to avoid or minimize the adverse effects of end-user errors. Chief among these is encryption of sensitive information on laptops, as well as other removable media and backup drives (PriceWaterhouseCoopers, 2008). Additionally, organizations are increasing the use of web content filtering, web site certification and accreditation, and secure browsers.

The SANS Institute's suggested Acceptable Use Policy for computer end-users states that "Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>'s Confidential Information policy when engaged in blogging." (SANS, 2006, p. 4).

But this general policy, while a good idea, is much harder to implement on a daily basis. First, users should be encouraged and constantly reminded to be careful what information they publish online and how they protect it. No one is immune to the tendency to divulge too much, as illustrated by the example of Sir John Sawers's wife. Not all of us are spouses of intelligence agency directors, but still many people put way too much private information in online postings and then fail to protect it adequately.

Security in social media sites starts with knowing to whom one is communicating. Many people have friends and followings online, but do not really know who their online "friends" are, or whether they are even who they claim to be. It is relatively easy for an attacker to impersonate someone in a social media site, for financial gain, defamation, or to collect information. In 2009, a Los Angeles screenwriter tried, as an experiment, to impersonate Sarah Palin in a Facebook account (Rosman, 2009). Within minutes of posting the account, he had over 100 friend requests. Within a week after the real Sarah Palin announced she was resigning as governor of Alaska, the account had over 600 friends. Some even offered to send donations, which the author never accepted.

In order to avoid disclosing information to an imposter, users should follow some prudent practices when communicating on social media sites. Primarily, users should

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

exercise basic caution when communicating and sharing information with online friends (Timm & Perez, 2010). Just as users are advised in security awareness training to disregard suspicious emails, they should follow the same advice with regard to requests for information on social media sites. If requested for information, they might call or email the requester to verify the request is genuine. They might also search for multiple profiles for the person, some of which might be imposters. A company can help ensure there are not imposter sites set up for it as well. It could accomplish this by monitoring social media sites for imposter accounts for the company and for the company's senior executives. It might also help employees monitor their social media profiles for imposter accounts.

Users should also carefully control what information they post on social media accounts and to whom this information is available. This particularly applies to users who actively participate on social media sites as part of their company job function, in order to network with customers and promote brand awareness. For example, Facebook's default settings make quite of lot of information that users post on their profiles available to everyone. By default, information that the user includes in their "About me" description, Personal Info such as interests and activities, family members and relatives, education and work, and all posts made by the user are visible to all Facebook users.

Even if users and companies try to protect their privacy by restricting the visibility of their personal information and posts on social media, the privacy policy of social media sites may undercut this intent. Users therefore should be very cautious what they post in social media sites. For example, in 2009 Facebook changed its terms of service to allow the company to retain archived copies of user content, even if the user had removed the content from their profile (Wikipedia, 2011). Following widespread criticism, Facebook reverted back to the original terms but stated it was in the process of developing a new set of terms with input from users.

5.5. Safe Browsing Practices Mitigate XSS And CSRF Threats

The other major social media threats that were cited in the Secure Enterprise 2.0 Forum report, XSS, CSRF, injection flaws, and insufficient anti-automation, are largely related to vulnerabilities in the web application itself, rather than to end-user behavior.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Nevertheless, with XSS and CSRF at least, there are some end-user practices that can help prevent attacks.

To help avert XSS attacks, end-users can use a combination of web browser settings and good browsing practices (Timm & Perez, 2010). First, they can disable scripting and active content in their browser unless it is absolutely needed. Javascript, VBScript, and ActiveX are common mechanisms used to execute XSS attacks. Users should also disable cookies if possible, as these often are used by sites to store sensitive personal data that might be stolen by an attacker.

There are also steps that the organization can take to help avert XSS attacks. These include installing desktop firewalls and application layer firewalls, network intrusion prevention systems, web content filters, and application layer proxies. Additionally, web site developers can help ensure that XSS vulnerabilities are not inadvertently built in to their applications, through the use of automated vulnerability scans and manual code reviews.

Similar safe browsing practices, such as disabling active content and scripting, can help avert CSRF attacks. Additionally, end-users can avoid setting up the required conditions for a CSRF attack. This means they should not be connected to a secure site, such as a financial institution web site, and another site at the same time. They should also avoid staying on secure sites longer than necessary, and be sure to properly log out before visiting other sites or closing their browser.

6. Security Policy? What Security Policy?

The preceding sections have attempted to show that the most serious threats to users and organizations can be mitigated through proper and consistent end-user practices. They have also attempted to show that such practices would be introduced and encouraged in a good security awareness program, and enforced in organizational security policies.

But organizational security policies do not always exist, and those that do are often out of date. According to a global study, 23 percent of IT professionals reported they worked for a company that did not have security policies (Cisco, 2008).

Maxwell Chi, maxwell.chi@sbcglobal.net

© 2011 SANS Institute, Author retains full rights.

Furthermore, 47 percent of end-users and 77 percent of IT professionals reported that their companies' security policies needed improvement or updating.

Another problem is that having a policy is one thing, while getting users to follow it is something else entirely. According to a global study, 56 percent of IT staff reported that security policies were briefed to new employees at the time of hire, but only 32 percent of employees reported having been briefed (Cisco, 2008a). Additionally, even when users are aware of security policies, they often disregard them in order to accomplish what they want. Wesley College in Melbourne, Australia, prohibits students from accessing social media because of security concerns and to prevent students from viewing inappropriate content. But the IT staff there reports that students are extremely good at circumventing this policy by setting up anonymous proxies (Gillis, 2010). In the U.S., 44 percent of workers admit they adhere to corporate security policies most of the time or less often (Cisco, 2008b). More than half of workers who have modified the security settings on their company laptops, did so in order to view web sites that were prohibited by their companies.

IT staff may be frustrated by end-users' failure to comply with security policies. But many end-users feel their organizations' security policies are outdated to the point of hindering their ability to do their jobs efficiently. In a global survey, 42 percent of workers reported the main reason they did not follow security policies was that the policies restricted them from using the tools and resources they needed to do their jobs (Cisco, 2008a). At one time, the workplace may have been ahead of many individuals in terms of cutting-edge technology, but today, it is often individuals who have left the workplace behind. Corporate IT resources and policies have too often not kept up with the marketplace (Gillis, 2010). Many employees therefore procure their own tools and create their own IT resources using modern technology, including social media tools.

Preventing workers from using updated technologies to which they are accustomed, can hurt the organization by stifling innovation, reducing efficiency, causing worker resentment, and increasing employee turnover. Many organizations restrict use of social media because they are concerned about information leakage, as well as damage to the organization's reputation from employees' actions online. The key for an organization is not to try to cut off employees from modern technologies, but to keep

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

its security policies updated and its employees properly educated on security requirements.

Security policies must reflect modern technologies and business processes. But all policies are toothless without effective enforcement. Many companies know their traditional security tools are weak and out of date, and are regularly circumvented by users in a rush to get things done. They reluctantly accept this behavior, knowing in any case that there is little they can do to prevent it. Organizations need a new set of tools suited to the modern business environment of social media and mobile, always-connected applications. But these tools must be transparent to end-users and support, rather than interfere with, performance of their jobs. Security tools that help, or are at least transparent to, end-users are more likely to be accepted.

Fortunately, next-generation security tools are becoming available, from leading networking companies. Emerging security tools and architectures are network-based, rather than platform-based (Gillis, 2010). Instead of having an individual antivirus scanner running on every PC or mobile device, a powerful, multicore scanner runs on the network. IT staff ensure that every device that connects to the network is directed at a network scanner. Because the security software runs on powerful network appliances, it can include not only malware scanning but also policy enforcement at the application and content level with very fine granularity and no additional latency. This type of security would help mitigate threats associated with malware and information leakage.

Social media includes a much larger number of access points than traditional wireless networks. Therefore, security software would be running on a variety of networking devices across the network, and yet the policies and enforcement would be uniform across the network because it is controlled by a central policy server with dynamic, continually updated information. Such tools, combined with proper security policies and end-user training, can enable organizations to reap the business benefits of social media.

7. Conclusion

Despite their advantages to workers and business processes, many organizations are reluctant to adopt social media technologies because of security concerns. Over half

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

of organizations worldwide prohibit the use of social media in the office. But increasingly, workers are demanding to be allowed to use these technologies to conduct business and collaborate with coworkers. When organizational policies prohibit the use of these technologies, workers simply circumvent the policies. Organizations feel powerless to prevent this behavior. Moreover, companies cannot continue to ignore the clear benefits that social media provide in productivity and worker morale, particularly as more of their competitors start adopting social media in their business processes.

There needs to be a shift in the view that many organizations have toward social media and security. Instead of attempting to develop new policies specifically for each new technology, organizations can develop and implement proper security policies and end-user training programs that are broadly applicable. The same general behaviors that protect end-users in when using the traditional Internet and email are effective in mitigating major social media threats as well. Organizations also need to enforce their policies by investing in updated security tools that are suited for the social media environment.

Maxwell Chi, maxwell.chi@sbcglobal.net

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

References

Baker, Adam. (October 2009). Phishing scams continue to plague social media sites. Wise Bread. Retrieved April 22, 2011, from World Wide Web: http://www.wisebread.com/phishing-scams-continue-to-plague-social-media-sites

Brodie, Cindy. (January 2009). The importance of security awareness training. SANS Institute Reading Room. Retrieved April 8, 2011, from World Wide Web: http://www.sans.org/reading_room/whitepapers/awareness/importance-security-awareness-training_33013

Burns, Jesse. (July 2007). Cross site request forgery: An introduction to a common web application weakness. ISEC Partners. Retrieved April 28, 2011, from World Wide Web: http://www.isecpartners.com/files/CSRF_Paper.pdf

Cisco Systems. (2008a). Data leakage worldwide: The effectiveness of security policies. Retrieved May 12, 2011, from World Wide Web: http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-503131.pdf

Cisco Systems. (2008b). Data leakage worldwide: The effectiveness of corporate security policies. Retrieved May 12, 2011, from World Wide Web: http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/Cisco_STL_Data_Leakage_2008_.pdf

Evans, Michael. (July 2009). Wife of Sir John Sawers, the future head of MI6, in Facebook security alert. Timesonline. Retrieved May 11, 2011, from World Wide Web: http://technology.timesonline.co.uk/tol/news/tech_and_web/article6644199.ece

Financial Times Lexicon. (2011). Social media. Retrieved June 22, 2011, from World Wide Web: http://lexicon.ft.com/Term?term=social-media

Fisher, Dennis. (May 2011). Phishing, social networking attacks on the rise. Threatpost. Retrieved July 11, 2011, from World Wide Web: http://threatpost.com/en_us/blogs/phishing-social-networking-attacks-rise-051211

Fraser, M. & Dutta, S. (February 2009). Web 2.0: Security threat to your company? SC Magazine. Retrieved February 27, 2011 from World Wide Web:

Maxwell Chi, maxwell.chi@sbcglobal.net

© 2011 SANS Institute, Author retains full rights.

http://www.scmagazineus.com/web-20-security-threat-to-your-company/article/127417/#

Frieden, Terry. (January 2009). VA will pay $20 million to settle lawsuit over stolen laptop's data. CNN.com. Retrieved May 16, 2011, from World Wide Web: http://articles.cnn.com/2009-01-27/politics/va.data.theft_1_laptop-personal-data-single-veteran?_s=PM:POLITICS

Gaudin, Sharon. (October 2009). Study: 54 percent of companies ban Facebook, Twitter at work. Computerworld. Retrieved February 22, 2011 from World Wide Web: http://www.wired.com/epicenter/2009/10/study-54-of-companies-ban-facebook-twitter-at-work/#

Gillis, Tom. (2010). Securing the borderless network: Security for the Web 2.0 world. Indianapolis, IN: Cisco Press.

Gordon, Josh. (n.d.). The coming change in social media business applications: Separating the biz from the buzz. Social Media Today. Retrieved May 26, 2010 from World Wide Web: socialmediatoday.com/ClientFiles/.../ SMT_whitepaper_biz.pdf

Hirschhorn, Karen. (January 2007). Insider Hacker Activity. IT Defense Magazine. Retrieved May 16, 2011, from World Wide Web: https://www.vericept.com/ Downloads/ NewsArticles/news_pdf_06/Insider%20Hacker.pdf

McKinsey & Company. (September 2009). How companies are benefiting from Web 2.0: McKinsey global survey results. McKinsey & Company. Retrieved March 30, 2011 from World Wide Web: http://www.mckinseyquarterly.com/ How_companies_are_benefiting_from_Web_20_McKinsey_Global_Survey_Results_2432

Perez, Sarah. (February 2009). Top 8 Web 2.0 security threats. ReadWrite Enterprise. Retrieved March 9, 2011, from World Wide Web: http://www.readwriteweb.com/enterprise/2009/02/top-8-web-20-security-threats.php

PriceWaterhouseCoopers. (2008). The global state of information security. Retrieved May 16, 2011, from World Wide Web: https://www.pwc.com/en_BE/be/ publications/information-security-survey-pwc-08.pdf

Maxwell Chi, maxwell.chi@sbcglobal.net

© 2011 SANS Institute, Author retains full rights.

Rosman, Katherine. (August 2009). Sarah Palin's Facebook alter-ego gets found out. The Wall Street Journal. Retrieved May 3, 2011, from World Wide Web: http://blogs.wsj.com/speakeasy/2009/08/13/sarah-palins-facebook-alter-ego-gets-found-out/

Rubin, Courtney. (October 2010a). Is social media really worth your time? Inc. magazine. Retrieved March 2, 2011 from World Wide Web: http://www.inc.com/news/articles/2010/10/small-businesses-conflicted-about-social-media.html#

Rubin, Courtney. (October 2010b). Is the online information about your business correct? Inc. magazine. Retrieved March 2, 2011 from World Wide Web: http://www.inc.com/news/articles/2010/10/consumers-more-likely-to-use-businesses-active-on-social-media.html#

SANS Institute. (2006). InfoSec acceptable use policy. Retrieved May 11, 2011, from World Wide Web: http://www.sans.org/security-resources/ policies/ Acceptable_Use_Policy.pdf

SANS Institute. (n.d.). Password policy. Retrieved July 11, 2011, from World Wide Web: http://www.sans.org/security-resources/policies/Password_Policy.pdf

Satyanarayana, Ashwin. (January 2009). Five security risks of social networking websites. Bright Hub. Retrieved March 30, 2011 from World Wide Web: http://www.brighthub.com/computing/enterprise-security/articles/9732.aspx

Schachtman, Noah. (July 2009). Military may ban Twitter, Facebook as security 'headaches'. Wired.com. Retrieved May 25, 2010, from World Wide Web: http://www.wired.com/dangerroom/2009/07/military-may-ban-twitter-facebook-as-security-headaches/

Schroeder, Stan. (February 2010). Social networks are becoming a security risk [SURVEY]. Retrieved February 25, 2011 from World Wide Web: http://mashable.com/2010/02/01/social-networks-security-risk/#

Schroder, Ashley. (March 2009). Magento CSRF attack: A simple explanation. Retrieved April 28, 2011, from World Wide Web: http://www.aschroder.com/2009/03/magento-csrf-attack-explanation/

Maxwell Chi, maxwell.chi@sbcglobal.net

© 2011 SANS Institute, Author retains full rights.

Sophos (February 2010). Malware and spam rise 70% on social networks, security report reveals. Retrieved July 11, 2011, from World Wide Web: http://www.sophos.com/en-us/press-office/press-releases/2010/02/security-report-2010.aspx

Timm, C. & Perez, R. (2010). Seven deadliest social network attacks. Burlington, MA: Syngress Publishing, Inc.

Waxer, Cindy. (February 2011). CIOs Struggle With Social Media's Security Risks. Public CIO. Retrieved March 3, 2011 from World Wide Web: http://www.govtech.com/pcio/CIOs-Social-Media-Security-Risks-021111.html

Webroot Software, Inc. (February 2010). New Webroot survey shows Web 2.0 is top security threat to SMBs in 2010. Retrieved March 8, 2011, from World Wide Web: http://pr.webroot.com/En_US/ about-press-room-press-releases-web-2-0-is-top-security-threat-to-SMBs-in-2010.html

Wikipedia (July, 2011). Criticism of Facebook. Retrieved July 11, 2011, from World Wide Web: http://en.wikipedia.org/wiki/ Criticism_of_Facebook#Terms_of_Use_controversy

Zeller, Bill. (September 2008). Popular websites vulnerable to cross-site request forgery attacks. Retrieved April 27, 2008, from World Wide Web: http://www.freedom-to-tinker.com/blog/wzeller/popular-websites-vulnerable-cross-site-request-forgery-attacks

Maxwell Chi, maxwell.chi@sbcglobal.net

© 2011 SANS Institute, Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced