SOCIAL MEDIA SECURITY MITIGATIONS

Version 1.1

12/3/2009

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0		*05/22/2009*			Initial Draft
1.1		*07/30/2009*			

TABLE OF CONTENTS

1 INTRODUCTION

Social media sites and other Web 2.0 technologies, such as Facebook, YouTube and Twitter, offer health communicators powerful new channels to deliver relevant and targeted health messages, often facilitated through trusted sources, when, where and how users want information. Since these technologies are newly emerging and are unfortunately prone to security vulnerabilities and attack vectors, mitigating these risks to protect the CDC network remains paramount to the Office of the Chief Information Security Officer (OCISO) and the programs alike.

Risks associated with social media sites may be classified into two main realms: the risk associated with CDC content hosted on these sites (social media sites as systems); and risks to the CDC networks from staff using these sites for official or personal reasons (social media sites as vectors). This document focuses mainly on social media sites as vectors and mitigating the risks to the CDC network. However, some recommendations such as password policies, incident response plans, and security concerns such as malicious applications, overlap both realms.

Many groups within the federal government are working to address the various security issues associated with social networking sites. For social media sites viewed as systems, NIST has adapted SP 800-53 Rev 3 to make allowances for accrediting hosted services where agencies are afforded limited or no negotiations, such as free services like Twitter and YouTube. A draft report to the federal CIO Council by the Web 2.0 Security Working Group addresses more of the issues with social media sites as vector. This document is intended to be CDC specific guidelines and recommendations, and as such may not be applicable for other agencies or organizations. Furthermore, since the landscape is constantly shifting, the recommendations and risks mentioned in this document are only as good as the latest draft and should not be considered exhaustive or comprehensive. As we learn more from our colleagues, we will regularly update this document to reflect the best practices to secure CDC's network and still uphold our public health mission.

Social media sites are not, for the most part, any more or less inherently insecure than other types of Web application sites. Technical vulnerabilities such as cross-site scripting (XSS), SQL Injection, and header splitting are the same across all web applications. The mitigations for all such systems are essentially the same. Application security communities, such as OWASP, do an excellent job of classifying and documenting these vulnerabilities, as well as educating developers on ways to secure their systems. Social media sites raise the profile and the stakes for attackers to exploit these vulnerabilities. One unique risk associated with social media sites that differentiate them from other Web applications is information leakage, mainly in the form of personal information which can be used for social engineering attacks (spear-phishing / 'whaling', architecting attacks for specific high-profile individuals, etc.) or used to compromise personnel in the traditional espionage manner.

The use of social media sites at CDC increases risk to CDC systems and data via four main mechanisms: 1) Web mail communication; which by-passes enterprise mail filtering, 2) public comments on blog posts; which are particularly vulnerable to cross-site scripting or spear-phishing attacks, 3) malicious 'friends'; whereby those who are accepted as ‘friends’, may change their profiles after being approved to purposely include malicious code, spurious, offensive, inappropriate or political content, and 4) malicious applications.

This document aims to outline the steps of risk assessment for individual sites and recommendations for mitigating these known risks when they are present.

In an internal policy recommendation, OCISO makes two general recommendations regarding social media sites and the first two main vulnerability classes:

- Do not use the Web mail portion of these sites.
- Disable comments on blogs and other public commenting sections.

This document will address these four classes of vulnerabilities from a business need/health communication aspect and make recommendations on how to mitigate these risks when the use of Web mail and comments are warranted as well as newly emerging risks of malicious friends and malicious applications.

2 VULNERABILITY CLASSES

2.1 Web Mail:

Most functions of social media sites are usually available even when Web mail is not used or is blocked by Websense. When feasible, this is the recommended route, not only in terms of security but also convenience. A possible mitigation technique would be to have incoming mail automatically redirected to a specific "group" CDC account. This would allow the regular enterprise mail filters to scan all of the incoming mail traffic; therefore providing the same level of security present with existing CDC enterprise mail accounts.

If Web mail is required to effectively use the site, then a computer off the CDC network will have to be used to manage and maintain the site. This requires separate hardware and connection to the Internet to be approved and secured by OCISO.

2.2 Public Comments:

OCISO recommends that comments be disabled by citing that even moderated comments pose a risk to the CDC network. Each of the submitted comments has to be opened and evaluated by someone on a CDC network computer, thereby placing the moderator's system in jeopardy. Using this method, there is no foreseeable way to moderate these comments without this risk present.

However, to not allow comments on blog posts and other web content is not only contrary to the very nature of these peer-to-peer communications platforms, but it reduces the site's effectiveness, and often generates a negative backlash which undermines the effectiveness of our communications efforts.

Public comments may also contain links to false locations designed for CDC staff to follow in a directed attempt to infiltrate the CDC network. These attacks are called spear-phishing attacks since they are aimed at specific individuals or classes of individuals. Sites that use URL redirection services, such as TinyURL, are particularly hard to secure. The uses of such services are commonplace in Twitter and other micro blogging sites where character count is at a premium. Extreme caution must be maintained when following such links or accepting comments that contain such links.

From a communications perspective, we recommend allowing comments, but having all comments moderated. A special computer off the CDC network will be required to manage and maintain the site. This necessitates the purchase of separate hardware and connection to the Internet to be approved and secured by OCISO.

2.3 Malicious 'Friends':

Once friends are approved on a social media profile, vigilance is required to make sure that the friend's profile hasn't changed to include inappropriate content, an inappropriate profile image or malicious code. The simple act of reviewing proposed friends may make the administrator's system vulnerable to attack. Although most users of such social media site already understand this, disclaimers about friends and content on their profiles should be posted. Clear policies about accepting friends should be posted as well. Some sites such as MySpace allow you to control which friends get listed on your main profile page, whereas others such as Facebook randomly place any of your friends on the main page, in which case, care must be taken in approving friends.

This vulnerability is the same as attacks whereby developers work to get a site high in Google or other search engine results, and then change the content of their pages to purposely introduce attacks.

Again, the main recommendation is to use computer resources off the CDC network to manage and maintain the profile. This requires separate hardware and connection to the Internet.

2.4 Malicious Applications:

Many social networking sites such as Facebook and LinkedIn allow for third party applications to be embedded on the profile pages. These applications pose a risk, as they have in the past been used to relay malware or are purposefully engineered to be used for attacks. Two main security concerns around the use of third party applications are the use of them by CDC staff while visiting these sites and the risk that if embedded on official CDC pages, then we unwittingly aid in an attack on our visitors. User training and appropriate adherence to rules of behavior can greatly mitigate the former. As for the latter, the inclusion of third party applications on official profile pages is not recommended unless the application provider can be trusted, eg, other governmental agency or well-known commercial vendor.

3 PRIMARY RECOMMENDATIONS

3.1 General Recommendations:

Since most Web 2.0 technologies are still emerging and secure coding practices are not industry-wide, it is recommended to do a risk assessment for each social media, Web 2.0 community you wish to use for official CDC communications. This assessment is to determine whether Web mail and public comments are allowed or even necessary. Most times they are either required or greatly preferred, and in those cases the only way to currently protect the CDC network is to manage and maintain these sites on hardware off the CDC network.

Programs must work to control those aspects of security that they can control. If a social media site does not require strong password policies, the program developed and OCISO approved Rules of Behavior (ROB) should contain strong password policies and policies on frequency of changing the password. Written Incident Response Plans (IRP) should be developed to handle possible compromises of passwords, data/site disfiguration, etc., which state what to do, who to contact internally (OCISO, DeHM) and externally (account managers at social media site, security at social media site, etc) as well as having prepared media inquiry responses for why the agency is involved in the channel, what we do to mitigate the risks, how we're working to get the problem resolved and so on.

Programs must work with OCISO to develop and implement appropriate Rules of Behavior (ROB) for those who will use the special hardware to manage these profiles. These ROB will include provisions of not connecting the hardware to the CDC network, trying to re-enable ports if OCISO has blocked them, or moving files from the system to the network directly in any way. Special connections to the Internet must be acquired, which is usually a wireless Internet card. If DSL, cable or T1 connections are required, then the program must also include ITSO in on the discussions at an early stage.

Programs should develop a system to regularly and systematically review the URLs in any comment for XSS on the destination. Those who do the scanning and review should be trained on how to look for suspicious XSS type of code in a page. The uses of automated tools are generally restricted by license agreements.

Programs should also develop a system too regularly and systematically review the profile pages of friends as well, to ensure that content has not changed since initial acceptance and that those profiles have not been compromised.

Programs should also routinely scan the security environment and vulnerabilities databases to stay breast of the changing security landscape associated with these sites.

3.2 System Definition and Boundaries:

Until these sites can be made more secure across the board, it is not recommended at this time to treat the information published to these systems as information of record or official. Disclaimers should be made on the profiles of each of these sites to state that official CDC information can be found at CDC.gov and that in the case of any discrepancies that the content on CDC.gov be considered correct. Even though clear system boundaries are established, programs participating in the spaces must assume the risk that content may be subject to attack and change, since ITSO and OCISO do not maintain these systems.

3.3 Data Collection and Communications Restriction:

It is prohibited to use these social networks to gather personal information or to be used for private or secure communications unless specific approval is granted in advance by OCISO.

APPENDIX A: REFERENCES AND RECOMMENDED READING

"Strategic recommendations for the secure use of Social Media within the Federal Government" Federal CIO Council, Information Security and Identity Management Committee, Network and Infrastructure Security Subcommittee, Web 2.0 Security Working Group. Version 0.4, July 23, 2009 Draft.

National Institute of Standards and Technology. ""NIST Special Publication 800-53 Revision 3." *NIST – Computer Security Resource Center,* August, 2009. Web. 1 Dec. 2009. <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf>

Wichers, Dave. "OWASP Top Ten Project." *OWASP Top 10*. 13 Nov. 2009. Web. 1 Dec. 2009. <http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Main>.

APPENDIX B: Specific site analyses and recommendations

MySpace: Since this site relies on Web mail to solicit and accept friends and the blog moderating functions have been known to have XSS vulnerabilities in the past, **it is recommended that to use this site for CDC communications, it be done so from specially designated hardware off the CDC network following guidelines developed in conjunction with OCISO.**

Facebook: Since this site allows blog posts and there is limited to no control over which of your friends appear on your home page, **it is recommended that to use this site for CDC communications, it be done so from specially designated hardware off the CDC network following guidelines developed in conjunction with OCISO.**

Twitter: An interesting site in terms of social media in that comments and posts are allowed, but are limited to 140 characters with no HTML or JS allowed. Hyperlinks are allowed and are automatically converted to the actual HTML code by the system. Eg – http://www.cdc.gov becomes <a href=http://www.cdc.gov>http://www.cdc.gov</a> automatically. Comments are designed to be sent by SMS messaging, which is text based. Requests for followers come through email and can be accepted without Web mail. Whereas it does seem to be secure against XSS exploits, the site does rely on AJAX technologies and can be used to post links to malicious sites. In order to vet these links, they must be followed, which would put the system at risk. The use of URL redirection sites is common in Twitter and is particularly vulnerable to phishing or spear-phishing attacks. **It is recommended that to use this site for CDC communications, it be done so from specially designated hardware off the CDC network following guidelines developed in conjunction with OCISO.**

DailyStrength: This site relies on Web mail to solicit and accept friends, allows blog comments and has limited to no control over which of your friends show up on your main profile page. **It is recommended that to use this site for CDC communications, it be done so from specially designated hardware off the CDC network following guidelines developed in conjunction with OCISO.**

YouTube: This site allows comments on videos and has limited to no control over which of your friends show up on your main profile page. **It is recommended that to use this site for CDC communications, it be done so from specially designated hardware off the CDC network following guidelines developed in conjunction with OCISO.**

Flickr: This site allows comments and has limited to no control over which of your friends show up on your main profile page. **It is recommended that to use this site for CDC communications, it be done so from specially designated hardware off the CDC network following guidelines developed in conjunction with OCISO.**

LinkedIn: This site relies on Web mail to solicit and accept friends and now allows for applications to be embedded in profile pages. **It is recommended that to use this site for CDC communications, it be done so from specially designated hardware off the CDC network following guidelines developed in conjunction with OCISO.**

APPENDIX C: Sample Social Media Usage Rules of Behavior (ROB)

Rules of Behavior for Social Media Usage

- I understand that I must complete role-based training at least once annually in order to obtain and maintain Social Media capabilities.
- I understand that I must not use computers connected or to be connected to the CDC Network to administer and maintain sites/profiles on social media sites.
- I will not store FIPS 199 moderate or high sensitivity data on the hard drive of any system not regularly connected to the CDC network. Contact program ISSO for assistance, or refer to http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf for guidance on data categorization.
- I understand that Social Media sites are non-secure systems and that no data will be passed from Social Media administration computers to the CDC network, except through the HHS email system or other mechanisms preapproved by my ISSO, OCISO and ITSO.
- I understand that even though certain Social Media administration computers may have limited port capabilities, I will not attempt to connect any of them to the CDC network.
- I agree to operate with security settings enabled by ITSO/OCISO to prevent compromise of systems or data.
- I understand that my login, when operating the Social Media administration computer, will be as regular user with **no** administrative privileges.
- I will run virus scans regularly.
- I will adhere to secure password guidelines as set forth by the agency, even if the Social Media site does not require that level of security.
- I understand that while logged in to Social Media sites I am in essence representing CDC and that I will abide by their respective rules of behavior and will not engage in any activities which may reflect poorly on CDC.
- I understand my responsibilities to protect systems and data as specified by CDC policies.

Protection of Information Resources
http://intraspn.cdc.gov/maso/policy/Doc/policy300.htm

Wireless Security http://intraspn.cdc.gov/maso/policy/Doc/policy447.htm

Use of CDC Information Technology Resources
http://intraspn.cdc.gov/maso/policy/Doc/policy90.htm

- I will report lost or stolen equipment immediately to CDC Physical Security Activity by e-mail at mailto:cdcsecurit@cdc.gov or by calling **(404) 639-3175**.

APPENDIX D: Social Media Site Profile Prelaunch Checklist

Social Media Site – Approval Checklist

1) Is content disclaimer and site ownership disclaimer in place?
2) Is there a plan for regular content updating and content review in place?
3) Is a blog comment moderation policy in place?
4) Has the staff responsible for creating and maintaining CDC content been briefed on the Social Media Rules of Behavior?
5) Is a plan for security vulnerability checks in place and staff assigned the review?
6) Has a written incident response plan been vetted and approved?

APPENDIX E: Routine Social Media Site Monitoring

1) Daily review of profile pages to ensure that content is still correct and hasn't been compromised.
2) Daily review of friends' photos and other non-CDC controlled content on profile page still fits within accepted guidelines.
3) Routinely check to see that friends' profiles are still in spirit as when they were originally accepted; that they are not advocating health practices not in keeping with CDC recommendations; that they are not advocating hate speech; that they are not advocating anti-governmental speech; that they are not baselessly critical of the administration; etc.
4) Routinely scan links to see that the destination pages have not been compromised or being used to promote attacks.
5) Routinely check on-line vulnerabilities reports for the sites you are using.

For regular review of reported vulnerabilities, you would access the databases at these three locations for vulnerabilities in the requested product. Be specific for the version being requested:

1. Vulnerabilities found in National Vulnerability Database (http://nvd.nist.gov/nvd.cfm)?
    - Click on the "vulnerabilities" tab and enter the name of the requested product.
    - If Vulnerabilities exist, they will be listed by date of submission

2. Vulnerabilities found in Security Focus Database (http://www.securityfocus.com)?
    - Click on the "vulnerabilities" tab
    - You will see a pull down for the "Vendors"; Search for the requested product (either by name or manufacturer)
    - In the event the requested product is not found, try inputting the name into the "Search field" (located in the upper right plain).
    - This will bring up results for the entire website (which may consist of various post and blogs concerning the topic)

3. Vulnerabilities found in Open Source Vulnerability Database (www.osvdb.org)?
    - Enter the requested products name in the "General Search" field located on the Upper Left Plain.
    - This will bring up any submitted vulnerabilities that have been submitted for the product.

Note: These entries are completed by users; therefore some of the entries may be incomplete. Often there are links posted within the page under "References" that will direct you to the posters source of information.