Social Media Vulnerabilities and Considerations for the Corporate Environment

Rob Hornbuckle

East Carolina University

Social networking is now one of the most dangerous security threats to an organization, according to recent studies by well-respected security firms such as Gartner, McAfee, and Norton. With over 1 billion people on Facebook alone, this will be a major threat for years to come. Hackers use this treasure trove of information freely provided by people about themselves and their companies to get the jump on many an organization. In fact, a recent study from McAfee has shown that half of organizations admit to a security breach resulting from social media in recent years. Consider also that only about a third of organizations have a response strategy or breach prevention policies when it comes to social media. This unchecked threat has the potential to not only wreak general havoc but can also be quite costly. While Facebook is the most notable social networking site, others to consider include: LinkedIn, Twitter, Yammer, MySpace, and Instagram. In an effort to mitigate this risk, all angles of vulnerability surrounding social media must be considered including: privacy attacks, malware distribution, data leakage, phishing attacks, identity theft, and evil twin attacks. Advanced attacks must also be considered including access-point spoofing, session hijacking, and targeted phishing attacks. Corporate practices can also be adjusted to better control response and prevention concerning social media attacks.

Globally speaking, privacy is a big concern in the United States but an even greater concern in Europe due to privacy specific legislation. It’s much easier to breech privacy laws in Europe than it is in the United States, which adds another component to a companies desire to protect information. Assuming an employee has their social media account hacked, a company can’t be held liable for the privacy loss an employee may incur surrounding the employees private information, but can get in trouble if corporate-specific data is involved in the data attacked. This idea is consistent with laws in the United States as well as in Europe. While protecting privacy on social media is of utmost concern, it is tricky as it all boils down to knowing the application and being educated about what information is appropriate to post. For instance, Facebook employs lots of privacy settings that can be setup to help protect its user base, however, they are in six different locations within the service. These almost hidden settings can be found in ‘Privacy’, ‘Timeline and Tagging’, ‘Ads’, ‘Apps’, ‘Blocking’, and in ‘Followers’. There are a lot of powerful settings to stop the transfer of sensitive information but knowledge as to how to appropriately set these options is required. Note that these privacy settings and policies are constantly being changed and updated as social media continues to evolve at a break neck pace. With this in mind, the safest course of action is to avoid posting sensitive information altogether. This is where employee training is most useful. Educating the employee base on the implications of their social media actions can be the most effective way to prevent attacks. While educating the employee base, its useful to discuss the implications of photos shared, photos tagged, and photo GPS, all of which have major issues revolving around privacy. With photo tagging a person can follow a chain of tags, referred to as a cluster, to find all people related to a person’s personal and/or professional life and potentially use this information to whatever ends they may. Consider the scenario where a competing company gains access to every company-depended engineer a competitor has through social media. This risk can be mitigated in privacy settings by disallowing oneself to be tagged in photos and then going back and removing oneself from all tagged photos. To complicate matters, many of these photos have imbedded GPS tags. Unless one manages these setting appropriately, most cell phones will embed the GPS quadrants from where the photo was taken and even embed the direction the camera was facing when the photo was taken. Using the information of where photos are taken and who happens to be in photos, a potential hacker can begin to form a picture of what ones life looks like, often including both personal and professional information. Unless you're a Kardashian and your livelihood depends on social media, it's just not reasonable to share this information with the public at large. Turn off the ability to be tagged in photos, turn off GPS imbedding, and encourage other employees to do the same.

Potential hackers consider social media an excellent vector to deploy malware attacks. Malware is malicious software that is installed on a computer to disrupt its proper function. The practical uses for malware are endless. Whatever motivation a hacker has, disrupting a company's network functionality hurts the bottom line. Typically, malware would be particularly hard to use, as the most successful attack vectors were limited to hacking known websites, which can prove difficult and time consuming. Social media, on the other hand, gives hackers a much easier vector for sending attacks. Gaming through social media is presently quite a large vulnerability. For instance, consider a Facebook user/company employee who loves to play Candy Crush on their lunch break and can't get past a particular level in the game and who receives an IM from a person advertising a 'walkthrough' for that particular level. That Facebook user is motivated to click on the link provided more so than they would an untargeted malicious email that contained malware. Through Facebook in particular, a hacker can obtain lists of people that belong to the same group to target their attack to a larger population, thereby increasing their chances of success. While attacks such as these are scary, the best defense is employee education. Employees must navigate carefully and be fully aware of the dangers of this type of activity. In addition, companies can consider blocking problem websites altogether if the problem persists.

Depending on the industry, the most worrisome and perhaps the most easily prevented vulnerability surrounding social media is data leakage. Employees must realize that nothing you put on a social media site should be considered secure or private. Even the computer geek who has every privacy setting enabled should still not assume all information is secure. Consider that the data posted is stored on the servers owned and/or controlled by the social media site. The user of the social media site isn't privy to the security of those servers nor can the security of the servers be guaranteed. While it is most likely buried in a disclosure, a social media subscriber can be assured that the social media site itself has been excluded from any liability resulting from a compromised server. Data also has the potential to be leaked every time a social media site updates or somehow changes the structure of its site or policies. Facebook as well as other social media sites are rapidly evolving and as such are subject to potential data leakage every time they alter their existing structure. While the most effective strategy is, again, employee education, DLP (data loss prevention) tools can be used to supplement existing strategy. Of particular note, DLP solutions can help shore up security in the case of a scenario where an employee unintentionally leaks data. A data loss prevention solution is a system that is inline with the companies network and/or client based that is designed to recognize patterns of data that would be harmful to the company if disseminated and subsequently blocks that information. Note that DLP solutions provide limited protection against intentional data leaks. The only strategy to protect against the scenario of a rogue employee is often a reactive one.

Another vulnerability to consider is identity theft. Identity theft is a real and serious problem in our country as well as abroad. While social media has its benefits, it only makes it easier to succeed at identity theft. Identity theft succeeds with minimal key information. Every bit of information one provides on a social networking site is excellent fodder for nefarious activity. Key information typically includes: name, date of birth, and address. Be assured that those who find a particular birthday relevant don’t need social media as a reminder. The best defense is to not provide any key information at all because, remember, nothing put on a social media site is secure or private. Corporations would be well served to educate their employee base against identity theft as untold havoc could result if a person can convincingly pose as an employee.

Social media users are also susceptible to what’s referred to as an ‘evil twin’ attack. An evil twin attack is an attack where an attacker creates a false social media identity based on the information publicly available on the target social media identity. For example, consider a scenario where a high-ranking executive in a corporation named John Richard Micon has established a LinkedIn account under John Richard Micon for professional uses. Next, a would be attacker has created a fake account in the name of JR Micon and copies all the public facing information on the legitimate account. The hacker then begins to add all the same contacts and if questioned responds that the other account had been hacked and that the JR Micon account was a replacement. The hacker can then use the vetted fake account to disseminate false information that could potentially hurt the victim or the employer of the victim. Evil twin attacks are difficult to defend against. They present a unique scenario where colleagues of an employee are the best defense against a successful attack. Employees will need to know what an evil twin attack is and how to spot it. Other options are more protective in nature. Consider actively monitoring high value employees online to spot and address potential vulnerabilities. It also might be worth claiming all variations of the names of high value employees in order to stifle a potential attack.

Most employees, especially those with public facing emails, are aware of phishing attacks as these types of attacks have been around for years. While they aren’t new, they do have social media as a new vector as most social media sites offer a message or mail system of some type. Defense against this type of attack relies primarily on employee education.

Advanced attacks using social media must also be considered, such as access point spoofing. Access point spoofing is an attack that isn't unique to social media. The simplest and sometimes most effective way to spoof an access point is to simply go to a location that offers free Wi-Fi, like a Starbucks for example, and then create a network name very similar to the original one posted. This can cause some users to use the spoofed network instead of the original one and provide much better access to sensitive data. This man in the middle position allows one to phish lots of data from user activity on the Internet. The biggest vulnerability here is with login IDs and cookies used to log into social media sites. If a phishing attack on a spoofed access point is successful and your login credentials are obtained, that malicious person can now access information unrestrained by even the most stringent security settings. Not only can they access all the information regardless of privacy setting but now have posting privileges. This type of unrestricted access can quite easily negatively affect the reputation of an organization. Note that nothing on a social media account is secure or private. Employee education must stress recognition of this type of attack. It's important for employees to speak up should they notice anything suspect when connecting to unfamiliar networks.

When an account is taken over in the manner illustrated above, it's referred to as session hijacking. While session hijacking can be accomplished through access point spoofing, it can also be accomplished by stealing the saved cookie from the computer itself. Using this cookie, one can log into your account without hassle. Beyond user education, defenses against this type of attack include use of services that require two-factor authentication when accessing from a new computer. For example, if enabled, Google will send a code via text message one must enter when accessing Gmail from a computer not previously used. Banks also commonly use two-factor authentication when they ask for answers to previously established security questions before completing login.

Another advanced attack worth noting is referred to as a targeted phishing attack. Targeted phishing attacks are like normal phishing attacks except an attacker will look through all social media data and tailor the attack specifically. There are companies that claim to have a 100% success rate in penetration testing against companies when using targeted phishing attacks. If this statistic isn't concerning enough, note that a phishing attack is just a vector for launching numerous attacks that are to a corporation's detriment such as: viruses, worms, data theft, data damage, and reputation damage. For example, a hacker has a look at a public Facebook profile and notices that an individual is not only the CEO of a company but has a number of friends in a local softball league and in particular talks a lot to another user, Jim. The hacker then creates an evil twin account posing as Jim. Next, he sends the CEO a Facebook email about the venue for the upcoming softball game. The email includes a hyperlink that looks like a legitimate softball venue but it is really a Trojan designed to search for company data on the CEO's computer and send it back to a specific computer controller by the hacker. One could very easily click this link and cause a data loss issue for the company, especially if the reproduction of the hyperlink is convincing, and be virtually undetected. The only true defense against targeted phishing attacks is to either not have a social media account, not have a social media account on your company machine, or not to click on anything within the social media account.

Company policy partnered with employee education is the best way to help protect an organization from the security vulnerabilities social media introduces. The only sure fire way to protect from social media in the work place is to prevent its use on any company machine. Now while this solution will prevent social media from causing problems it isn't practical for a large number of businesses as social media is quite a powerful marketing tool used to enhance brand image and is an effective tool used to manage corporate reputation. It can also have an effect on employee morale, more so with its removal than with its use. For these reasons, it's not often recommended to ban social media entirely, unless very high security is necessary or the company is part of a regulated industry. To that end, the start of any security in the realm of social media needs to begin with an acceptable use policy.

Acceptable use policy for social media will normally fall under acceptable use for computers and mobile devices. This policy will outline all the situations stated earlier and appropriate actions to take if the situation arises. This policy will also need to address security circumvention techniques. For example, tethering a G3 phone to a computer to bypass corporate security on a desktop or taking a laptop home and connecting at a Starbucks should be expressly prohibited. These same policies also need to address smartphones that have a connection back to the office, such as receiving company email on a company provided cell phone.

Policy is a great place to start but mistakes will still happen either from negligence, misconduct, or simple curiosity. Policy alone cannot fully protect a company from damages. A DLP (data loss protection) solution offers proactive protection and there are a few to choose from to suit an organization's needs. The difficultly in setting up a DLP is proper configuration without overloading the system with rules that would simply serve to cripple the use of any social media. This process can be both tedious and time consuming. To accomplish this, the DLP will need to be content-aware and data-centric within its function. The solution will also need to make decisions and act immediately on possible policy breaches. With a DLP in place, one can rest assured that company data has a second line of defense against loss. Also note that as a side bonus, most DLP solutions will also protect email traffic and file transfers from your office. A potential disadvantage to DLP solutions is that a DLP solution will not work with Apple or Android devices. Note that while DLP is a proactive solution, all companies will need to employ some sort of anti-virus software, which acts as a reactive solution to protect against loss.

Another solution that some companies have looked into is to setup a more secured social media outlet for its employees. A good example of this is Yammer. With better content control and a smaller user base to deal with you can reach some of the gains social media offers while managing some of the risks as well.

Social networking has forever changed the way we do business. It's a very powerful tool that can be used to not only improve the reputation of a company but also can serve to protect a company's reputation. The applications are endless from a marketing aspect as social media can be a springboard to advertise new products and generate substantial buzz, which can equate to large profits. From an HR aspect, social media can be utilized to enhance wellbeing and communication between the company and its employees as well as between employees. As such, social media isn't something we can cut out of professional life. Our workforce as a whole must adapt to mitigate the risks that social media presents if we are to take advantage of all the positives social media brings to the table. Adequate training, refined acceptable use policies, and a strong DLP solution are a must and they must evolve as social media evolves. Social media can be quite a weak point from a security aspect but managed correctly it can be a great asset.

References

Eridon, C. (2012, 09 14). 10 Social Media Risks MOST Companies Are Too Afraid to Take. Retrieved from http://blog.hubspot.com/blog/tabid/6307/bid/33579/10-Social-Media-Risks-MOST-Companies-Are-Too-Afraid-to-Take.aspx

Gonsalves, A. (2013, 11 04). Employees easily tricked on social media prime phishing attacks. Retrieved from http://www.csoonline.com/article/742639/employees-easily-tricked-on-social-media-prime-phishing-attacks

Hertzberg, J. (2013, 03 08). Managing Your Company's Social Media Risks. Retrieved from http://www.baselinemag.com/social-media/managing-your-companys-social-media-risks/

Kelly, N. (2013, 01 03). Social Media Risks Are Real, Not Managing Them is Irresponsible. Retrieved from http://www.socialmediaexplorer.com/online-public-relations/social-media-risks-are-real-not-managing-them-is-irresponsible/

*Kim, H. (2012, 07 01). Online social media networking and assessing its security risks. Retrieved from http://www.sersc.org/journals/IJSIA/vol6_no3_2012/2.pdf

Lanaarazie, I. (2010, 06 10). 5 Social Media Risks for Companies and Employees… And How To Prevent Them. Retrieved from http://socialtimes.com/5-social-media-risks-for-companies-and-employees-and-how-to-prevent-them_b14745

Lesnykh, A. (2012, 01 10). How CISOs Can Combat the Data Leak Risks of Corporate Social Media Access. Retrieved from http://www.itbusinessedge.com/cm/community/features/guestopinions/blog/how-cisos-can-combat-the-data-leak-risks-of-corporate-social-media-access/?cs=49479

Nerney, C. (2011, 05 31). 5 top social media security threats. Retrieved from http://www.networkworld.com/news/2011/053111-social-media-security.html

Peterson, D. (n.d.). How do you find the GPS coordinates of your photos? Retrieved from http://www.digital-photo-secrets.com/tip/1401/how-do-you-find-the-gps-coordinates-of-your-photos/

*Rauber, G. (n.d.). Privacy attacks in social media using photo tagging. Retrieved from http://precog.iiitd.edu.in/psosm_www2012/a4-pesce.pdf

*Sancho, D. (2009, 08 01). Security guide to social networks. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_security_guide_to_social_networks.pdf

Waxer, C. (2011, 02 11). CIOs Struggle With Social Media’s Security Risks. Retrieved from http://www.govtech.com/pcio/CIOs-Social-Media-Security-Risks-021111.html

Wells, S. (n.d.). Social Media Security Professional (SMSP) Training Course Overview. Retrieved from https://www.ultimateknowledge.com/_SMFREEWebinars.asp

*- Journal References