Microsoft

Social Networks and Enterprise Security

Effective Security Practices Series

The rise of social networking has brought with it a new crop of challenges for CISOs and security professionals. One looming concern is that employees may be revealing too much of their professional lives online. It might be a status update on Facebook about a "big project that isn't looking good" – a quick cross reference with some other posts might reveal what that project is. It could be a recommendation request on LinkedIn – this might signal an employee is looking for a job: are other people in their division looking too? Could the company or division be in trouble? This has become an important corporate security issue as tools and technologies are now available to correlate and visualize this data to infer confidential information. This whitepaper looks at some of the new threats, the state of data mining technologies, and some current effective practices to help manage the threat.

Herbert H. Thompson, Ph.D.
Chief Security Strategist, People Security

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA

Preface

Information security is a very dynamic field: legislation keeps changing, technology keeps evolving, and the attacker community continues to be more sophisticated. This turmoil has forced security practitioners to think creatively to address some very difficult problems. Much of this innovation has been locked away within corporations as they have made isolated progress on issues like security metrics, security risk management frameworks, and security policy. In order to address this discrepancy, Microsoft commissioned a whitepaper series to share key security innovations. Whitepaper topics came from participants in Microsoft's CSO Council - a semi-annual gathering of security executives from leading global organizations who serve as advisors to Microsoft's Trustworthy Computing Group.

Our goal is to share practices "from-the-trenches" that address some of the toughest problems in security. After numerous interviews, discussions, and debates with these though leaders, a collection of effective practices emerged. While much remains to be done, we hope that these whitepapers fuel the discussion and help facilitate further sharing in the field of IT security.

Overview

The rise of social networking is creating new information disclosure challenges for corporate CISOs. Individuals are revealing an increasing amount of information about both their personal and professional lives online. While the threat of talkative employees is not new, a perfect storm might be brewing. Consider the following:

Data creation: People are broadcasting more of their lives than ever before online. More than 55 million status updates are posted every day on Facebook alone. In late 2009, Twitter announced its 5 billionth "tweet", a 140 character message that answers the question "What are you doing?"

The Rise of Open Source Intelligence (OSINT) Tools: A new batch of Open Source Intelligence tools now exists to help map out people's lives and relationships. These tools give attackers, competitors, governments, and individuals the ability to correlate information across time and users.

Increased Credibility and Personalization of Phishing Attacks: A large volume of personal and business data online makes it easy for attackers to personalize phishing attacks and in some cases, automate the personalization process. Tools and frameworks now exist to gather enough information about an individual online to custom craft emails that include significant credibility information. This means that a glut of personal information online may put the business at risk by increasing the likelihood that an employee could fall for a scam that actually targets the business.

Limitations of Policy: Setting internal company policy can be a powerful tool to curb social network use during working hours. Setting policies to stop employees from using these social networking sites at work, however, does not stop them from talking about work when online at home. A broader approach is needed.

In combination, these factors highlight the need for businesses to carefully consider how to manage the risk that stems from social networks. In this paper we look at some of the emerging threats along with effective practices for businesses dealing with social networks.

The Threat of Corporate Information Disclosure

It might be an update about something personal like a restaurant they've just eaten at or a movie they're about to see. It might be news of moving to a new apartment. It may also be something work related, and it's at this point, the netherworld where work and home blend together, that this behavior starts to become a matter of corporate security.

Most employees that have access to sensitive corporate information are too savvy to disclose something important directly. Instead, they may accidentally divulge a piece of data that by itself is uninteresting, but when correlated with other posts, may lead to a significant disclosure of sensitive information. Consider for example the tweet (Twitter post): "Dealing with a crisis at work." By itself, this piece of information may seem harmless. From a social perspective it may inform friends that this person won't be available for the evening. For a viewer who is less interested in the person and more interested in their company however, this could be an important data point. What if some of their previous posts included things like "Spending all my time on this new account" and then weeks earlier "Check out the press release http://tinyurl.com/????, that's my account!" Any one of these three posts in isolation provides no sensitive information. Combining the three however could indicate that something bad has happened with a very specific customer. The consumers of this information might be broad: a competitor's sales department, other customers, investors, etc. Even more context might be gathered by looking at this person's LinkedIn profile (their position in the company, the division they work in, etc.) or from their colleagues and their information streams.

Another component to consider is the permanence of online conversations. A casual corporate disclosure to a friend over cappuccinos may go unnoticed – people eavesdropping around you don't have any context for the information such as who you work for or what your position is. In contrast, there is likely to be a record of everything a user has posted on their Facebook wall or Twitter stream over the past year which could potentially be mined.

Several CISOs interviewed during the writing of this paper indicated that a critical challenge in the next few years will be how to balance corporate confidentiality with the rapid increase of information sharing through social networks. This is a challenge that cannot fully be addressed through the normal corporate channels of setting policy. Something as simple as "don't talk about work online" is nebulous. Does a status update

on Facebook that you're in Bentonville, Arkansas, cross the line? Most people wouldn't think so, but the fact that your company is doing business with Wal-Mart (one of the only companies headquartered in Bentonville) matters.

Indirect disclosures are especially troublesome because they may appear to be harmless in isolation. This means that a normally prudent person may inadvertently reveal a piece of information that is the cornerstone of a serious breach of sensitive information when viewed in aggregate. These indirect disclosures may take the form of a relationship with another company (as shown on LinkedIn for example), a location that they may be traveling to for work, or it may be through job-seeking behavior which could indicate instability within a company or division when looked at across employees. Some specific types of indirect leakage to consider are:

Job-seeking behavior – If someone believes their job to be at risk it is natural to begin to posture for other employment. Consider, for example, typical pre-job-seeking behavior on one of the most popular business social networking sites, LinkedIn. The prospective job seeker may start updating their profile and may also reach out to colleagues for recommendations, and in-turn, offer recommendations to other co-workers, hoping for reciprocity. A rise in LinkedIn recommendations among rank-and-file employees may not indicate much other than general angst. At the executive level this behavior is more telling. Job-seeking behavior from several senior executives might reveal an impending closure, acquisition, merger, unfavorable earnings report, etc.

Relationships and Connections: Indirect information leakage may come from monitoring relationships and connections. Watching the LinkedIn or Facebook connections of people that work in Mergers and Acquisitions for a big company can be revealing (and are an obvious target), but the more telling disclosures come from clustering of relationships between senior employees at two companies. New visualization tools are available to help see and track these connections (more on this later). Every time an employee adds a business-related connection, they can help map out a piece of the puzzle. Blossoming relations between two companies might be a precursor to a new partnership, an acquisition, or a new client.

Location: Many people indiscriminately reveal where they are when they post on Twitter, Facebook, etc. Several successful social networking services like Loopt, Tripit and Doplr facilitate this. If you tweet about eating a sandwich and you're at home, this isn't very

interesting. Discussing business travel to smaller cities that house only one or two multinational companies like Bentonville, AR (Wal-Mart's headquarters) or Bloomington, IL (State Farm Insurance's headquarters) may indicate a budding business relationship. Tracking the blogs and Twitter streams of a company's sales force might allow a competitor to map out client names and sales strategies – the crown jewels of Sales and Marketing.

The challenge for an attacker or competitor has shifted from accessing sensitive information to mining meaningful items from huge volumes of data online.

The Age of Information Correlation

A wealth of personal information available online is not new. What is new, are the tools and technologies to help mine and correlate this information easily. These tools are part of a new breed of technologies referred to as Open Source Intelligence (OSINT) tools. Many in the technology community are accustomed to "open source" indicating the public availability if source code. In the case of Open Source Intelligence, the term refers to mining publicly available information to gather intelligence about a person, group, company or government. These OSINT tools help a user navigate through huge volumes of irrelevant information to zero in on related data and connections. Many of these tools provide the ability to visualize data and connections and then monitor these connections over time. Every additional piece of information posted online can help paint a more detailed picture of corporate and personal behavior.

Beyond special purpose tools, major search engines such as Bing and Google allow users to fine-tune searches more than ever before. These advances in both search and special purpose tools mean that businesses need to look at new lines of defense to protect sensitive corporate information and help employees make more security conscious decisions about the information they release online.

Defending the Enterprise

An employee can create a rapidly-growing digital footprint online. This demands new tactics to protect the enterprise. In discussing these issues with enterprise CISOs, we see a variety of new approaches being piloted. One approach is to use the tool of policy to

block social networking sites while at work. The primary motivation for blocking these sites is to stop time wasting at work; not to protect against information disclosure. More broadly, many have begun to investigate security awareness programs, which include sensitivity and awareness to information posted on social networking sites.

Education helps employees tap into growing awareness around privacy. Privacy, like security, is often ignored until an incident occurs and the risk is personalized. Awareness programs can help bridge the gap by bringing the threat to the forefront and putting it in a personal context. Large-scale awareness campaigns around privacy and online chattiness have begun to surface in recent years. Figure 1 for example shows a media campaign by Insafe, an EU backed organization that helps to promote internet safety to young people in Europe. The campaign included several videos that help to show the dangers of posting information online visually.

Figure 1 - An embarrassed animated mouse stands next to the warning "Think Before you Post." This image is part of a larger campaign of posters, videos and pictures created by Insafe, an EU backed organization that promotes internet safety to young people.

Security and privacy awareness campaigns can highlight threats and also discuss specific cases where information revealed online has led to some adverse corporate effect. It can also help to clarify confidentiality policies and map them to day-to-day activities online. Over the past year several companies, countries, and groups have started pushing privacy awareness. Figure 2 shows a public service announcement from a local newspaper in Nassau, Bahamas urging citizens to carefully consider what they post online.

Similar campaigns have begun to show up at both a corporate and national level. Several enterprise CISOs indicated they had plans to include social networking and potential

corporate risks as part of their future security awareness campaigns although few indicated that this content was integrated into current campaigns.

Figure 2 - A public service announcement from the Bahamas Telecommunication Corporation (a utility owned by the Bahamas Government) in local dialect urging citizens to be careful what they post on Facebook. Awareness campaigns such as this have begun to surface at both a national and corporate level.

The popularity of social networking applications will continue to grow and any potential risks to the enterprise must be managed. Some of the major social networking sites have launched security and awareness initiatives over the past year but these measures may be insufficient to defend enterprise interests. For example, the process of restricting information to a group of "friends" has shown to be of questionable effectiveness. A recent study by the Security firm Sophos puts the rate of "indiscriminate friending" – accepting friend requests from people you don't actually know – at near 40 percent. Security should not be left in the hands of a social networking company whose primary goal is to engage individuals more, not less.

Policies and education will be key defenses against the threat of intelligence gathering by both attackers and competitors. Fortunately, most employees that make indirect disclosures about their company do so without ill intent. This means that security education and awareness are important and potentially effective tools. Until security and privacy is woven into the fabric of social networking sites, corporations must help and motivate employees to make better decisions about the information they share online.