NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/news/2009/101909-baited-and-duped-on.html

Baited and duped on Facebook

By Mary Brandel, Computerworld
October 19, 2009 12:41 PM ET

When CIO Will Weider encouraged employees at Ministry Health Care and Affinity Health System in Wisconsin to use Facebook to spread the word about new programs and successful projects, he was surprised at the result: Few did so.

"I went in there thinking, 'We've turned these people loose; we'll have 10,000 marketers out there,' " Weider says. But the Ministry Health workforce, it turned out, had been well trained to protect sensitive data, and without explicit guidance on what they could say, their first reaction was to share nothing.

"We've stressed the importance of data security with our employees, particularly when it comes to patient privacy, and it's kept them from sharing all the great things about work on Facebook," Weider says.

That's a good problem to have. Many fear that the popularity of social networking -- among individuals as well as organizations -- will precipitate an increase in social engineering attacks that could result in security breaches that expose corporate data or damage a company's reputation.

Indeed, social media such as Facebook, LinkedIn, Twitter, online forums and blogs create a perfect opportunity for an attacker, mixing the anonymity of the Web, easy and direct access to hundreds of millions of people, and an unprecedented amount of personal information.

Consider that before social networking existed, criminals had to make a real effort to engage victims, says Adriel Desautels, chief technology officer at Netragard LLC, a security service provider that performs vulnerability assessments and penetration tests for clients. Often, the payoff wasn't worth it. But with social media, it's easy to hit a large number of targets quickly and effectively, he says.

"Instead of having to fool that one particular person, they can befriend a whole bunch of people," Desautels says. "They can post a URL on their wall, and one of those people is likely to click on it."

Approaching Storm

But while executives seem to grasp the potential threats of social networking, only a slim majority of organizations seem to feel the need to do something about it. In an exclusive September 2009 Computerworld survey, 53% of the 120 IT professionals polled reported that their organizations have a social media usage policy, while 41% said they don't and 6% said they weren't aware of such a policy.

And in a July 2009 poll by advertising agency Russell Herder and law firm Ethos Business Law, both based in Minneapolis, 81% of the 438 respondents said they have concerns about social media and its implications for both corporate security and reputation management. However, only one in three said that they have implemented social media guidelines, and only 10% said that they have undertaken related employee training.

A Deloitte LLPsurvey echoes those results. Only 15% of 500 executives polled said that the risks of social media are being addressed in the boardroom, although 58% said they agree that it's important to do so. But even those that do have policies may not effectively communicate them. Of 2,008 employees that Deloitte surveyed, 26% said their employers had guidelines regarding what they could say online, 24% said they didn't know if their employers had such a policy, and 11% said that there was a policy but they didn't know what it was.

Not that a policy covers every base, says Ira Winkler, a Computerworld.com columnist as well as the author of Spies Among Us (Wiley, 2005) and president of Internet Security Advisors Group, an IT security firm whose services include espionage simulations. But certainly a hands-off approach is no longer an option, nor is blocking the use of social sites at work.

"Too many companies want to say, 'That's your private life, so I won't bother you,' " he says. "But people's insecure behavior at home proliferates insecurity in the business."

The concern isn't just that employees will divulge sensitive data outright. It's that they'll reveal enough information about themselves or their workplaces -- either in one profile or distributed over several -- to enable an imposter to assess their personalities and gain their trust, figure out responses to their password-reset questions or convincingly pretend to be a co-worker, business partner or customer (see "How Hackers Find Your Weak Spots").

"Little pieces of information put together the big picture," Winkler says. Valuable tidbits include birth dates; the names of children, pets and best friends; facts about employers or comments about how projects at work are going; lists of hobbies; updates about vacations or life-changing events; and links to friends. The information is simple to find, either by using reconnaissance tools such as those available at sites like Maltego.com and Pipl.com or by simply doing searches on Facebook or LinkedIn.

When Netragard conducts penetration tests, it finds all the people on Facebook who work at a particular company and extracts data from their walls, posts and profiles. It pulls this information into a database and analyzes the results to assess things like the company's culture, whether someone will respond quickly to a request or how seriously security personnel take their jobs. From a simple comment about a Java register misbehaving again, Desautels says, Netragard can create an attack that looks like something the company won't notice or care about.

The bad news, Desautels says, is that there's no sure way to protect your company against social engineering threats. After all, the vulnerability stems from the natural human tendency to trust other people. However, there are measures you can take to reduce the risk that a hacker will succeed. A good place to start is with a social media policy.

Such policies range from strict to very liberal. For instance, sports broadcaster ESPN Inc.'s guidelines ban employees from setting up personal Web sites and blogs that contain sports content and requires workers to receive permission before engaging in any form of social networking dealing with sports.

Meanwhile, Ministry Health encourages employees to discuss positive work events and even to offer constructive criticism of their employer. However, it also has guidelines that, for example, prohibit employees from sharing patient information online under any circumstances, Weider says.

One basic but controversial policy question is whether to allow workers to mention their employer by name in their online profiles or in social networking forums. According to Desautels, prohibiting those practices is the best way to defend against social engineering threats.

If you're really concerned, you could consider restricting employees from providing their office e-mail addresses and identifying the geographic region in which they work, says Terry Gudaitis, cyberintelligence director at IT security firm Cyveillance. Even then, it's possible that a friend's comment or other conversations visible on an employee's profile could reveal employer information. In such a situation, it's up to the profile owner to monitor and delete those references, she says.

Similarly, Winkler suggests restricting employees from mentioning business developments on their profiles. What if, for example, a researcher discusses his lack of progress on a project or, perhaps even more revealing, a major breakthrough? Or if a salesperson tweets that she's meeting friends because she just won a big account? Combined with other information, such as names recently added to a salesperson's friend list, such tidbits can reveal quite a bit, Winkler says.

"This stuff used to be under lock and key in a private diary," Gudaitis agrees. "The amount of disclosure on every level -- business dealings, trade secrets, classified information and personal information -- is enormously high." Also alarming, she says, are employees who tweet during meetings about what's happening and even who's in attendance.

Of course, policies banning the mention of employers would take companies out of the marketing-on-social-media game. But Desautels cautions against that type of marketing anyway. "You'd be opening your customers to an entire world of potential hurt via phishing and other types of attacks," he says in his blog.

Weider, on the other hand, says not using social media for marketing is unthinkable. "Why don't we just stop publishing our phone numbers so people can't get into our voice-mail system, or lock our doors so the patients can't get in?" he says.

The way to avoid possible exposure, says Weider, is to establish clear data-security policies and offer employees ongoing training. That training could touch on ways to tighten the security settings on sites like Facebook. According to the Web site NextAdvisor.com, which compares online services, Facebook users should fine-tune who will have access to specific aspects of their profiles and posts using the "My Privacy" section of the site.

Not Too 'Friend'-ly

Companies may also want to advise employees to not accept every friend offer that comes along. "In a lot of cases, people say yes to anyone who pops up," says Gudaitis. "But then they're vulnerable to whoever those people may be." Better to be conservative, she says, and approve only business acquaintances or old college buddies or family members.

To be even more cautious, NextAdvisor says, you should even verify whether a friend request is from the person it appears to be from, by sending him an e-mail or calling him. "It is easy for someone to set up a phony profile

under the name of someone you know and trust in order to extract additional information from you," the site says.

Employees should also be aware that just because social networking sites ask them for personal information such as their birth date and phone numbers, it doesn't mean they need to provide it. In a poll of Facebook users that NextAdvisor conducted recently, 27% of respondents said that they listed their full name, date of birth, phone number and e-mail address in their profiles, and another 8% said that they included their street address as well.

"Your real friends and associates will likely already know this information, so including it on your profile will only increase your risk of being victimized by identity thieves," the site says.

Of course, hackers can collect that information even if you don't provide it all in one place. To guard against that, Gudaitis suggests varying your screen name.

Imagine, she says, if a hacker were able to track a specific systems administrator's or help desk technician's every move online, gathering information from message boards and forums, because the victim used the same screen name everywhere. "If I were an adversary, I could start to link all that information and even chat them up to better understand their network and system architecture," she says. "If we looked up every post someone had . . . we could put the puzzle pieces together."

Companies can also look inward at some of their own practices to close social engineering security gaps. In addition to advising employees to choose password-reset challenge questions that can't be answered through research, you could also follow Google Inc.'s leadand send password information to employees' cell phones instead of their e-mail addresses.

Hiring practices are another area in which security can be tightened. Winkler suggests screening the social networking habits of job candidates not just for stereotypical areas of concern, such as amoral behavior, but also for how active they are in social media and how likely they are to do things like expose personal information and voice extreme political views.

Perhaps most key, says Desautels, is designing your infrastructure and managing your sensitive data with an eye toward minimizing damage in the event of an intrusion. He stresses the importance of using encryption, recording and logging network activity, classifying data and putting your most sensitive data in a zone that can't be reached through the network. With a properly designed infrastructure, "you can keep a successful penetration from being successful in stealing your data," he says. "Just because they break in, they don't have to put you out of business."

In the end, it's really about finding a balanced way to leverage social media while minimizing risk, Weider says. For him, social engineering threats are certainly among his top 10 concerns, but they're nowhere near No. 1. "It's something I take seriously," he says, "but I do think there's a balance between reasonable risk and the likelihood of these various things taking place."

Brandel is a Computerworld contributing writer. Contact her at marybrandel@verizon.net.

For more enterprise computing news, visit Computerworld. Story copyright Computerworld, Inc.