CITADEL
INFORMATION GROUP, INC.

Protecting Your Business from Social Networking Attacks

Stan Stahl, Ph.D.
Kimberly Pease, CISSP

August 2009

Sally, the accounting manager of Acme Enterprises, a medium-sized business, regularly checked her Facebook account while at work. One day she received an email. The email said that a long-lost friend, Bob, had added her as a friend in Facebook. There was a link in the email for Sally to follow to confirm the friend request. Sally clicked the link. Over the next week, cyber-thieves withdrew nearly $1,000,000 from her employers' bank account.

Welcome to the newest nastiest twist in cybercrime.

You see, the email wasn't from Bob and the link didn't go back to Facebook. Bob's on Facebook just like Sally is. That's how the cyber-thieves found them and discovered that they might know each other. That's also where they learned that Sally worked in the accounting department.

After that it was a simple matter to set the trap by sending Sally a friend request from Bob. "How great," thought Sally, "an email from Bob. Let me just follow this link and we can be friends again."

Link followed. Trojan horse installed. $1,000,000 stolen.

According to Breach Security, the number of web security incidents was up 30 percent in the first half of 2009. And social networking sites like Facebook, MySpace and Twitter were the target of 19% of all attacks, more than any other category. That's a big change from last year's report when government networks were the most often attacked and social networks weren't even on the list.

Making matters worse, many of these attacks succeed by taking advantage of missing patches and using obscure technology like "0-day exploits" that get past traditional antivirus and antispyware defenses.

As if that's not bad enough, businesses shouldn't expect their banks to cover losses. Regulation E of the Federal Deposit Insurance Corporation (FDIC) stipulates consumers are protected by cyber crime involving their banks. The FDIC regulation does not cover businesses, however.

Here are five things you can do to inoculate your business against social network attacks:

1. Prohibit use of social network sites from the office. These sites can be blocked at the corporate firewall. This can become particularly challenging if employees work remotely as it may not be feasible to block access to social networks from home computers.

Making matters worse, Trojan horses are like communicable diseases and Sally's work-at-home computer can be infected from her son's. That's why the next four recommendations are so important.

2. In addition to antivirus / antispyware defenses, add advanced defenses like intrusion detection and prevention designed to block internet-based attacks like the link in Sally's email and 0-day exploits.
3. Your IT staff can block known internet-based attacks by comparing links against a database of known bad links like http://stopbadware.org/home/reportsearch.
4. Keep your systems patched. This means not just Windows patching but all your applications, those you know about — like Office and Adobe Reader — and those you might not even know about — like Flash and Java. This also includes your Macintosh computers as they are every-bit as vulnerability-prone as Windows PCs.
5. Finally, don't expect to rely on technology alone. Users are often the weakest link so it's very important to train them to detect the subtle signs of an attack so they can keep from becoming victims. They also need to be given guidance on what information is safe to put on a social networking site. Sally put a big bulls-eye on her back when she wrote that she works in Acme's accounting department.

There is no one thing you can do to keep from being victimized from a social network attack. Even doing all five of these isn't a guarantee, just like a flu shot doesn't guarantee you won't get the flu. But if you are diligent you can significantly affect the odds and this should be your objective.