Workplace Service

First Cut
Number: 2012-FC9
June 7, 2012

Aragon Research

Topics: Workplace, Social Software
Issues: What technologies and architectures should enterprises leverage in the workplace?
What are the best practices for leveraging social software to gain a competitive advantage?

Author: Jim Lundy

LinkedIn Security Breach Reinforces Need to Secure Social Networks and Content

***Summary**: Hackers defeated security measures and stole 6.5 million passwords at LinkedIn. Enterprises should evaluate their use of public social networks and the security that cloud providers offer.*

Event: On June 6th, 2012, LinkedIn confirmed that 6.46 million LinkedIn users' passwords had been stolen and posted online. This follows attacks earlier this year on Facebook in the UK, in which a worm called Ramnit was used to steal 45,000 user passwords.

Analysis: Public social networks such as LinkedIn and Facebook are now being used as cyber-war attack vectors, and most of them are not secure enough to withstand these sophisticated attacks. The exploits range from brute-force password theft to sophisticated Advanced Persistent Threats that target specific individuals who use public social networks.

The ultimate goal of such an attack is to take over PCs, smartphones or tablets and get sensitive personal, corporate or government information from them. The most disturbing news is that these attacks are being made not only by individual hackers but also by governments (state sponsored attacks).

In the case of LinkedIn, the passwords themselves were inadequately protected (a process called *salting*), but there are a myriad of ways to attack cloud-based applications, with Instant Message payloads being one of the most popular.

The frequency and pace of such attacks is increasing. Enterprises must re-evaluate their strategies with regard to specific applications such as social networks, and also how they evaluate SaaS and PaaS providers.

Cloud providers are not standing still. It is clear that Google has learned some strong lessons from their experience of being hacked by the Chinese (see Note 1). Google is now alerting users if they appear to be the subject of a state sponsored attack (see Note 2). This implies that Google has added extra monitoring layers to their cloud infrastructure, something others will have to do.

Enterprises need to do several things in light of these increasingly frequent attacks. A three-pronged strategy is needed to look at tools, cloud providers and critical content/information and where it is located.

First, **do not share work-related information on public social networks**. Use them only for advertising and marketing, but not for substantive collaboration. This includes Facebook and other consumer social networks (see Research Note 2011-12, "In a World of Cyber-Espionage, Facebook is Not a Friend of Your Enterprise").

Second, enterprises and governments need to **increase due diligence about the services**

that cloud providers offer. From now on, many cloud providers will have to do more than just the occasional security scan. **Real-time threat monitoring is a must**; a growing number of companies offer the extra layers of protection that you need (see Note 3).

Last, and most importantly, state-sponsored attacks generally have specific information targets. Enterprises and governments need to **identify and classify their critical content** and secure it to minimize the risk of loss. Targeted information includes:

- Product designs
- Engineering drawings
- Product launch plans
- Source code for software products
- Password control system access

The only sure way to secure this kind of content is to store it offline, or at least off of an Internet-connected network. Organizations must categorize and classify their content and identify the information that needs the greatest protection.

Aragon Advisory

Don't use public social network sites at work. Especially in high-risk and high-sensitivity arenas, create a separate network to provide suitable protection.

Cloud providers must constantly adjust to changing threats. Before contracting with a provider, carefully evaluate their security, information protection, and ability to monitor for malicious activity.

Passwords and password security are often managed far too casually. **Both policy and active enforcement are needed to require strong passwords and the necessary periodic changes for ongoing protection.**

Notes

Note 1: In January 2010 Google described their detection of a highly sophisticated attack on their infrastructure that resulted in the theft of intellectual property. The attack targeted not just Google but more than twenty other companies. Responding to the threat, Google strengthened their infrastructure security, and advised users to take action with anti-virus and anti-spyware software of their own.

Note 2: Google employs numerous security audits and tracking services to monitor for malicious activity. When they suspect that an individual may be the target of a state-sponsored attack, they display a warning banner to that effect.

Note 3: Increasingly, security providers offer real-time threat intelligence, typically cloud-based. These services monitor a network for threats across their potential lifecycle (from initial exposure to actual attack) and deliver notifications and triggers for action. Representative providers include Symantec, McAfee, RSA, IBM, and ArcSight.