A Cloud Security Breach? It Can't Happen to Me!

By Taiye Lambo

June 2012

Recent Events in Cyber Security

Just recently, some 8 million users of the high-profile social networks LinkedIn and eHarmony had their passwords compromised in a major security breach. A hacker publicly posted lists of these passwords on the website InsidePro for the entire world to see. For many cloud security experts, these recent events are no surprise. However for many of us who are users of cloud based services from companies like Google, Facebook, Dropbox, and Amazon, these very public security violations should be a wakeup call: breaches can happen to you and you should be prepared.

Even the informed consumer of cloud services often have misconceptions of what a security breach entails and how to protect against one. In the early days of the Internet, websites were discrete, easily distinguishable nodes with little interconnection and data was largely stored on physically separate servers. Major security and privacy concerns around keeping data confidential, maintaining its integrity, and ensuring its availability were relatively simple. However, with the advent of cloud computing, these security challenges have morphed in ways that we are often not aware of when we sign up for and utilize cloud based services.

Understanding the Full Scope

For all the benefits the cloud has brought us, it has also greatly increased the stakes in cyber security. When a single cloud service provider gets breached, it can impact individuals across industries, countries, and backgrounds. Yet, a breach of one cloud service can and most likely will affect a multitude of other cloud services. For example, the username to most cloud service providers is your primary email address. Although, as of the time of this article's writing, the list of usernames for LinkedIn and eHarmony were not released publically, they are most certainly retained by the hackers.

Do you have a unique password for your LinkedIn account? What about Facebook? Or Gmail? If not, a hacker who has access to your username and password for one cloud based service can likely now access not only all the information stored on the breached service (which could be extremely confidential personally or professionally) but can use your login credentials to access sensitive information on other cloud based services. Considering that many of us use browsers that auto-store our passwords, it can be quite difficult to determine which additional services may have been compromised as a secondary result of the primary security breach.

Primary and Secondary Damages

If a cloud based service like Facebook is breached, a hacker can gain unlawful access to your service account page. The, information here includes Personally Identifiable Information (PII) such as your date of birth, home address, telephone number, and possibly your payment information all stored within such a cloud based service – information that is often used to verify your identity on other third-party websites. This alone can lead to cases

of identity theft. More malicious hackers known as Black Hats can additionally utilize your personal content like private pictures and messages to damage your reputation. One common next line of attack is to use whatever content is obtained from the breached cloud based service to engage in phishing attacks. We already see reports of LinkedIn users receiving official-looking emails asking them to change their passwords. This allows hackers to gain even more sensitive information or direct users to inappropriate or malicious content.

Another step commonly employed by hackers is to focus on leveraging a first breach to gain entry into a second service or network. These secondary breaches can even be more damaging than the first. If your username and password are shared across several cloud based services such as the OpenID Single Sign-On Framework, a hacker can, and likely will, access these additional services. This can include accessing your online banking information, insurance healthcare benefits, iTunes account, messaging programs, personal and work email accounts, online storage accounts, and others. It's a scary thought just to consider all the sensitive information that's available just in your email inbox, let alone the rest of these cloud-based services.

For a website like LinkedIn, which is used by many corporations' Human Resources department as a tool for recruiting, compromised login credentials can potentially be used to access other online systems that provide access to health information, background checks, legal and court documents, or cause of termination for a whole host of employees. Given that many Department of Defense and other government agencies use LinkedIn as well, these major concerns take an even more serious tone regarding national security and confidentiality of classified documents. After all, it is not difficult for hackers to locate the relevant internet facing systems such as webmail servers and attempt to access such information using usernames and passwords compromised elsewhere.

Proper Password Management:

It is incumbent upon the CIOs (Chief Information Officers) and CISOs (Chief Information Security Officers) to ensure the highest possible levels of protection for their customers' information by implementing holistic information security management standards, such as the ISO 27001, and also getting an independent CloudeAssurance rating for the cloud based services that they consume. However, as we have seen by these recent events, consumers of cloud services cannot rely strictly on the service providers to protect their privacy and security.

Here are four simple steps you can take to improve the security of your cloud based services. They are extremely straightforward, but even the vast majority of tech savvy consumers fail to take them fully into account.

1. Create a personal password classification scheme. Use different login credentials for cloud-based applications like Facebook and LinkedIn and your work-related environments.

2. Change your passwords regularly and ensure you avoid common terms and phrases including elements of your biographical information, use complex alphanumeric passwords consisting of special characters, upper and lower case letters whenever possible.
3. Utilize passphrases instead of passwords by forming acronyms for a phrase that you will be certain to remember. This builds barriers to easy password cracking.
4. Set up a designated email address to sign up for cloud based services, especially those you are not very familiar with: this reduces the amount of spam and phishing and forms a protective wall if your security is compromised on any of these services.

Some cloud experts recommend using cloud based password safes, or downloaded programs that store passwords for several websites and allow you to input a single master password. While such cloud based services are extremely convenient, they are increasingly becoming targets for malicious hackers. As such, the safest course of action is to utilize the four aforementioned strategies and thereby take your cloud security into your own hands.

About the Author: Taiye Lambo is a seasoned entrepreneur with Global Information Security and Governance, Risk Management and Compliance expertise with a focus on Cloud Computing. He is the Founder of USA based CloudeAssurance, Inc. – www.CloudeAssurance.com, eFortresses, Inc., the Holistic Information Security Practitioner Institute (HISPI) and the UK Chapter of the Honeynet Project and can be contacted via e-mail (tlambo@eFortresses.com) or *LinkedIn (http://www.linkedin.com/in/taiyelambo).*