PUBLICATION

Living in the Clouds: Is Your Business Data at Risk Because of a Disgruntled Employee?

Authors: Jordan Tyler Corbitt
July 12, 2017

TheCloud: Good Morning! TheCloud is a leading cloud-based provider, striving to secure your apps, email and confidential data in the cloud. How may we help you today?

Mr. Techie: My name is Mr. TechieTechie, I'm the CEO and founder of Tech to Tech. I have an account with TheCloud, but I'm having trouble accessing it all of the sudden. It keeps saying the password is incorrect.

TheCloud: I see, and what is your account number?

Mr. Techie: 7264388. I had access to the account just two days ago. What changed?

TheCloud: It appears that the primary contact on the account, Mr. Disgruntled, logged in yesterday and made some changes to the account, including changing the network password.

Mr. Techie: Mr. Disgruntled hasn't worked here in six months! How is he able to do that?

TheCloud: When the account was activated, it appears that you designated Mr. Disgruntled as the primary contact on the account, which enables him to make changes, including changes to login information. The primary contact also has access to company data, and is able to send and receive emails.

Mr. Techie: Well as I mentioned, Mr. Disgruntled was terminated more than six months ago, and he no longer is authorized on this account. Please delete Mr. Disgruntled as the primary contact and replace him with me.

TheCloud: Unfortunately, Mr. Techie, we are unable to do that. As primary contact, Mr. Disgruntled essentially owns the account and its content. Any changes that are made must be authorized by him.

Mr. Techie: I'm the CEO and founder of the company. Are you telling me that I'm locked out of my own account? And the only way I can get back in is with Mr. Disgruntled's permission? That's ridiculous. *I own the account!*

TheCloud: That's right. And unfortunately, since you are not authorized on the account, that is all of the information I can provide you with today. Please have a pleasant weekend! **Try not to think about Mr. Disgruntled destroying your data, contacting your customers and stealing your proprietary information! Buh-bye!**

"Click." Of course, a dutiful customer service representative would never let that last part slip. However, three days later, you realize that Mr. Disgruntled has indeed misrepresented to potential customers that he is still in charge of the company. He is taking orders and promising customers that their orders will arrive without delay. But they never get their orders, and a customer has now called you explaining that because her order never got there, she has lost $1,000,000 in revenue. Needless to say, she is upset, and using you as a supplier in her future business plans is the last thought on her mind.

More and more it is becoming glaringly obvious that one of the largest threats to a company's security is disgruntled ex-employees. According to a warning issued by both the FBI and Department of Homeland Security (DHS), there has been an increase in computer network exploitation and disruption by unhappy or former employees. The FBI and DHS warn that "the theft of proprietary information in many of these incidents was facilitated through the use of cloud storage websites and personal email accounts." Companies who fall prey to cyber-attacks by disgruntled employees suffer significant costs, ranging from $3,000 to $5,000,000. The FBI and DHS recommend various actions that can thwart a hacker's plan to wreak havoc:

- Conduct a regular review of employee access and terminate any account that individuals do not need to perform their daily job responsibilities.
- Terminate all accounts associated with an employee or contractor immediately upon dismissal.
- Change administrative passwords to servers and networks following the release of IT personnel.
- Avoid using shared usernames and passwords for remote desktop protocol.
- Do not use the same login and password for multiple platforms, servers or networks.
- Ensure third-party service companies providing email or customer support know that an employee has been terminated.
- Restrict Internet access on corporate computers to cloud storage websites.
- Do not allow employees to download unauthorized remote login applications on corporate computers.
- Maintain daily backups of all computer networks and servers.
- Require employees change passwords to corporate accounts regularly (in many instances, default passwords are provided by IT staff and are never changed).

Congress has also done its part to help protect computer data. In 1996, Congress amended the Computer Fraud and Abuse Act (CFAA), broadening the CFAA to protect computer data from theft on any computer used in interstate commerce. In 2001, Congress again broadened the CFAA's reach to any computer "located outside the United States that is used in a manner that affects interstate or foreign commerce or communication in the United States." The CFAA focuses on punishing those, via criminal and civil liability, who "access[es] a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter." Moreover, there are numerous state laws protecting electronically-stored information that employers should be aware of, ready to utilize them when the occasion arises.

Employers are now equipped to handle disgruntled employees' attempts to commandeer employer's proprietary information, but the trick is addressing this issue before the employee becomes disgruntled. But how? First, all employment agreements, offer letters and/or employee handbooks should specify that authorization to any company account or other electronically-stored information is prohibited after the termination of the employment. Second, only employees who are trustworthy and long-term should have the ability to change login information or other account settings. Finally, companies must be proactive. When an employee is terminated, their access to company accounts must be terminated as well. In an age where technology is necessary to achieve greatness, it is imperative to not let that same technology be the reason for a company's failure.