Egnyte Security Tips for Small – Medium Businesses

Keeping Business Data Safe

Security, it's the number one concern of businesses when adopting new technologies involving company data. Due to the recent data center security breaches on several large companies, data security against unwanted intrusions is on everyone's mind. Why do these attacks happen and what can businesses do to protect themselves?

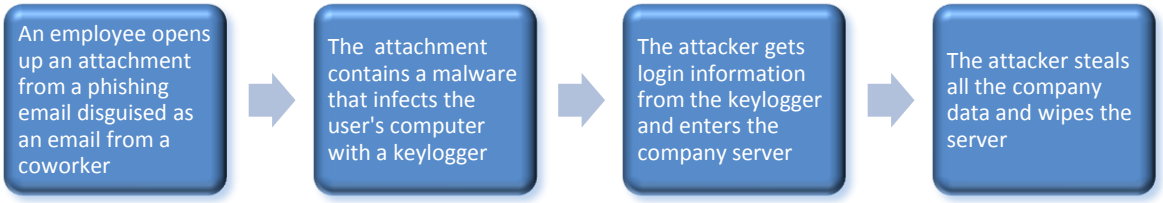
Intruders Eyeing Small Businesses

If there's one thing recent data breach headlines have taught us, it's that attackers aren't always motivated by monetary gain. Data breaches may be motivated by data theft, political opposition, company sabotage, blackmail or to just malicious intent to kill off a business. Even though some of these attacks can be complex in nature, the majority of attacks are simple routine intrusions aimed at easy victims.

Security studies have proven that government agencies and large corporations are becoming increasingly difficult for intruders to breach. Recent cybercriminal arrests by the U.S. Secret Service have deterred intruders from large-scale high-risk attacks. This leads cybercriminals to the focus on easier targets: **small businesses**. Smaller-sized businesses often cannot afford enterprise-class data security systems, leaving them easy prey for attackers looking for a quick score. Unlike major corporations, small businesses often don't survive a cyber attack.

How Data Breach Happens

You go into work one morning, turn on your computer, click on the company folder and you see… nothing. All the information is gone; client files, logs, billing information have all been compromised. Your business just became a victim of a data breach cyber attack. So what happened?



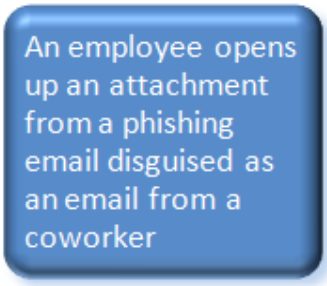
The chart shows the process of a typical attack on a small business. The bad news is that an attack such as this one is simple to execute. The good news is that this attack could have been easily prevented. According to the "Verizon 2011 Data Breach Investigations Report", 92% of all data breaches in 2010 were of low difficulty and 96% of those attacks were avoidable through simple or intermediate controls[1].

The average common data intrusion attack takes several days to complete. That gives plenty of time for system administrators to stop the attack. An observant business knows how to react to the attack at any point of the intrusion. A secure business can prevent these attacks from happening in the first place.

[1] Verizon 2011 Data Breach Investigations Report: Page 4, "What commonalities exist?"

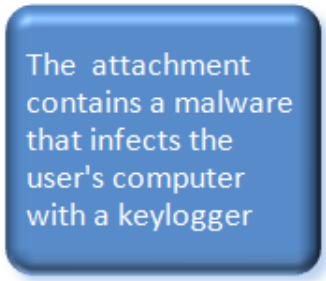
Protecting Your Data

Breaking down the attack process in the previous example shows what businesses can do to prevent each stage of the attack and what action to take if it already happened. IT departments should ensure their business has all the following preventative and reactionary measures in their company infrastructure.



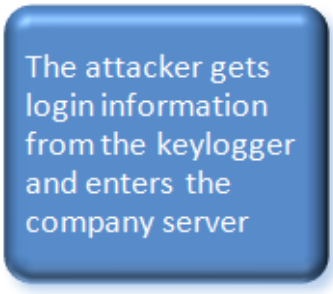
Prevention: Education – Businesses should educate their employees on best practices regarding external internet sources. Inform employees to download files from emails and links only if they are completely sure of the source.

Action: Containment – Once an unknown file is downloaded, the first step is to delete the file. Then disconnect the computer from the network and have IT run a complete system sweep to ensure no traces are left.



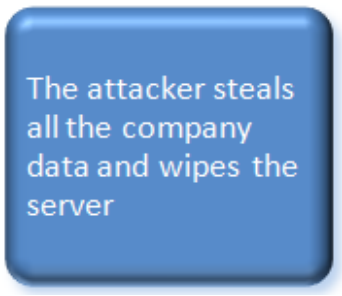
Prevention: Virus Scan – Every computer connected to the company network should be equipped with updated virus detection systems. Virus scanners should be able to detect and delete harmful programs the second they enter the computer.

Action: Password Management – Keyloggers are spyware programs that track user keystrokes to obtain login/password information. Once a keylogger is detected on a computer, IT should immediately reset passwords on all related accounts.



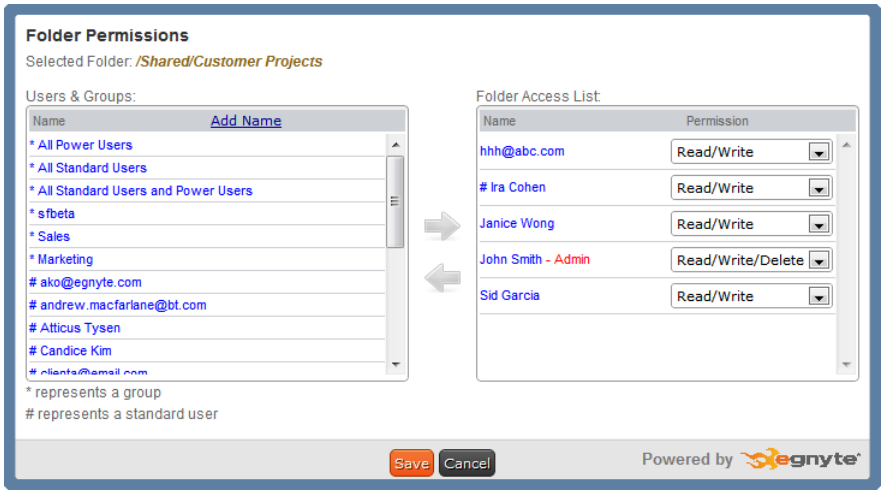
Prevention: Central Administration – Businesses should have central administration capabilities on their local and cloud server. Controlling which users have access to what files/folders on the server ensures that essential business data is only accessible by authorized individuals.

Action: Disconnect – If an unwanted user is caught accessing the file server, disconnect them. Businesses should be diligent in detecting and reporting unusual user activity. Always play it safe. If an unknown user is entering the server remotely, disconnect first, ask later.



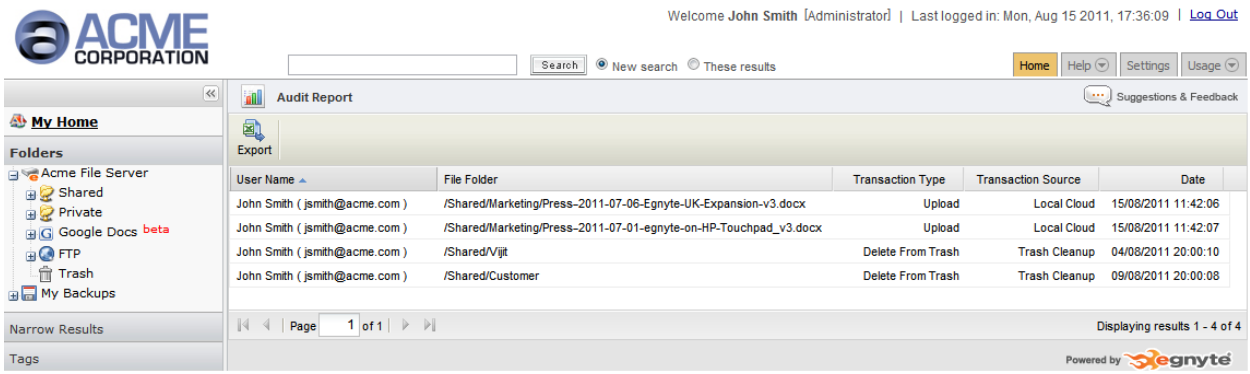
Prevention: Audit Report – Comprehensive local and cloud server services offer live audit reporting on file usage. IT should always monitor and track file/folder access based on users. Catching suspicious activity in the system ensures that data breaches are caught before any major damage is done.

Action: File Backup – Have all business files backed up in a remote cloud server. If disaster recovery is necessary, all files backed up in the cloud can be imported back to the local server to prevent complete data loss.



Left: Example of Egnyte Local Cloud Central Administration. File and folder access permissions are set by the Admin.

Bottom: Example of Egnyte Local Cloud Audit Report. Used to track and monitor file/folder usage based on user, transaction, and time.



Conclusion

Data breach is becoming a major concern as more businesses adopt data storage technology. Cybercriminals are seizing this opportunity to attack vulnerable businesses unfamiliar with data security. Most small business cyber attacks are simple in nature, but extremely effective against networks that don't practice basic security protocols. The first step for any businesses should be to understand the fundamental stages of a cyber attack. Then the business should adopt proactive measures to prevent intrusions as well as reactive measures to stop attacks.

Over 1 Billion files shared by businesses using Egnyte HybridCloud File Server. Egnyte's unique HybridCloud technology provides the speed and security of local storage with the flexible accessibility of the cloud. Users can easily store, share, access and backup files, while IT has the centralized administration and control to enforce business policies. Egnyte, founded in 2007, is based in Mountain View, California and is a privately held company backed by venture capital firms Kleiner Perkins Caufield & Byers, Floodgate Fund, and Polaris Venture Partners. For more information, please visit www.egnyte.com or call 1-877-7EGNYTE.

Egnyte Inc. | 1890 N. Shoreline Blvd., 1st Floor | Mountain View, CA 94043, USA | Phone: 877-7EGNYTE (877-734-6983)
www.egnyte.com | © 2011 by Egnyte Inc. All rights reserved. | Revised September 2011