EventLog Analyzer helps First Mountain Bank stay Compliant with The Federal Deposit Insurance Corporation (FDIC) Audit Requirements

OVERVIEW

Industry
Banking

Critical Requirements
- To meet Federal Deposit Insurance Corporation (FDIC) Audit Requirements
- Real-time Notification during anomalous network activities without having to log into a monitor console (Push technology)
- Scheduled reports (daily, weekly, monthly) to designated users

Solution
ManageEngine EventLog Analyzer

Results
- Mitigated risk of security breaches
- Real-time alerts during anomalous activities
- Reports for review emailed to various groups on defined schedules
- Compliant with FDIC audit requirements

> "Windows Event logs and device Syslogs are a real time synopsis of what is happening on a computer or network. EventLog Analyzer is an economical, functional and easy-to-utilize tool that allows me to know what is going on in the network by pushing alerts and reports, both in real time and scheduled. It is a premium software Intrusion Detection System application."

Jim Lloyd,
Information Systems Manager,
First Mountain Bank.

The Customer

First Mountain Bank is a full service community bank serving the mountain and high desert communities of San Bernardino County, California, with offices in Big Bear Lake, Running Springs, and Lucerne Valley. The Bank opened for business in October 1981 with one office in Big Bear Lake. The Bank's original and ongoing mission has been to serve the banking needs of the Big Bear Valley and surrounding communities.

The Bank provides customers with a broad range of products and services including real estate construction financing, commercial real estate and home loans, consumer loans and business lines of credit, along with a variety of checking and savings products.

The Challenges

The objective of a financial institution is to be able to manage customer money and be a profitable business. It has to be done in the most secure way possible. Money is the object of greed and therefore attracts those who want to take it for themselves. Money is no longer solely retained in a physical vault. It is travelling electronically from one place to another. It only takes knowing personally identifiable information about a person to take their money. Financial institutions also have to retain that information. If not properly secured, that data can be compromised allowing money to be stolen from anywhere in the world. Financial institutions stand to lose a lot of money very quickly if the appropriate security measures are not in place. Just as one would put an alarm on their home to try and stop a thief that is trying to break in to a building, Intrusion Detection Systems (IDS) can provide warnings of an attempt to gain access to a network.

Data, system and network security has become an ever increasing and major Information Technology and Information Systems focus. Hackers and exploiters have become increasingly savvy over time in being able to compromise company, client and person information. Better

hardware, software and knowledge is required to provide the ability to protect that data and the networks it resides and travels on from malicious intrusions.

Most business level hardware and software products provide real time data output of their operation. Windows operating systems, routers and network switches produce log events of everything they do, but they don't usually provide a meaningful way to do anything with it. The sheer volume of information that can be produced can be overwhelming and impossible to review, much less in real time. They can be set up to send these outputs to a device that collect, collate, and take action on them in an automated fashion.

Since the events of September 11, 2001, financial institutions have been required to increase their levels of security in all aspects of their operation. The FDIC (Federal Deposit Insurance Corporation) coordinates federal level standards and audits to help regulate financial institutions. Guidance is driven by requirements of Homeland Security and provided by such organizations as FFIEC (Federal Financial Institutions Examination Council) and NIST (National Institute of Standards and Technology) Special Publications 800 series publications. Not only is there a systemic need to have this level of security, but there is also a governing body that is expecting it.

The Management of First Mountain Bank was facing the challenge in 2008 of staying compliant with its independent auditors and the Federal Deposit Insurance Corporation (FDIC) compliance audit requirements. Auditors and the FDIC directly and regularly examine and supervise all banks in the U.S. for operational compliance, safety and soundness. FDIC Compliance is important to maintain insurance certification for any bank, as well as the cost, and proof of security has become paramount. First Mountain Bank needed to develop higher security standards.

The Resolution

Jim Lloyd, Information Systems Manager at First Mountain Bank reviewed several products that would satisfy the needs of the bank, and fit the FDIC requirements to be compliant. Verbally assuring an auditor or examiner about a security process is not sufficient. First Mountain Bank had to show readable compliance reports during these audits that proved acceptable security measures were in place and working. Using the free version of EventLog Analyzer, a few key servers were set up and a number of events set up to provide proof of concept. The next audit validated EventLog Analyzer's viability with a report comment that the bank would benefit from all of its devices being monitored.

Since 2009, EventLog Analyzer has been providing the bank with continued operation and has grown to over 250 individual alert items and some 15 weekly activity reports. It is a mature application requiring only periodic changes over time. "I don't need to be in the application to know if something is happening that needs attention. I get reports and alerts through emails. No surprises when I walk into the office. That is peace of mind." says Jim Lloyd, Information Systems Manager at First Mountain Bank

A Final Note

Here are just a few requisites Jim Lloyd suggests to get any person started with EventLog Analyzer in monitoring network security:

- Security events in Windows Vista and in Windows Server 2008
  http://support.microsoft.com/kb/947226
- Security Monitoring and Attack Detection
  http://technet.microsoft.com/library/Cc875806
- Watch your system event logs for events specific to your environment.

About EventLog Analyzer

EventLog Analyzer is a web based, real time, agent less (optional agent available), event log and application log monitoring and management software. EventLog Analyzer helps monitoring internal threats to the enterprise IT resources and tighten security policies in the enterprise.

http://blogs.eventloganalyzer.com/ www.facebook.com/LogAnalyzer https://twitter.com/LogGuru

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization's need for real-time services and support. Worldwide, more than 60,000 established and emerging enterprises — including more than 60 percent of the Fortune 500 — rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with offices worldwide, including the United States, United Kingdom, India, Japan and China.

http://blogs.manageengine.com www.facebook.com/manageengine https://twitter.com/manageengine