Indirect Taxation Authority of Bosnia & Herzegovina Boosts Network Security and Streamlines Log Management with EventLog Analyzer

OVERVIEW

Industry

Government

Critical Requirements

- Streamline log management in a highly distributed network environment
- Centrally monitor Syslog & Windows EventLog data from network devices and systems
- Mitigate Internal threats

Solution

ManageEngine EventLog Analyzer

Results

- Streamlined log management by automating log collection, monitoring and reporting
- Seamless, centralized collection of Syslog & Windows EventLog data from network devices and systems
- Mitigated risk of security breaches by tracking user activities in real-time

Company Information

Indirect Taxation Authority (ITA) of Bosnia and Herzegovina was established at the end of the 2003 and is tasked with developing and maintaining a unique value added tax system in Bosnia and Herzegovina. It is practically the biggest state level institution responsible for taxation and customs in Bosnia and Herzegovina. The Headquarters of Indirect Taxation Authority is in Banja Luka. The field activities are run by four regional centers in: Sarajevo, Banja Luka, Mostar and Tuzla, 30 customs sub-offices and 59 customs posts, out of which 40 are passenger border crossings, 4 airports, 8 railway border crossings, 3 overseas mail offices and 4 free zones. The organizational structure of the Indirect Taxation Authority is the following: five sectors and four departments comprising the Office of the Director.

Challenges

The IT department of Indirect Taxation Authority (ITA) located at the headquarter is the central point linking to all other Indirect Taxation Authority's regional offices and organizational units spread throughout Bosnia and Herzegovina. The IT network at Indirect Taxation Authority is a highly distributed environment consisting of over 90 different servers, 2300 workstation computers running on Linux/UNIX and Windows platforms accessed by 3500+ users at 80 locations throughout Bosnia and Herzegovina.

The IT department was facing the challenge of managing the log data generated by their distributed IT network consisting of a central HQ, 4 regional centers and more than 50 remote Customs locations connected over WAN. ITA knew that their log data was the primary source that would provide security intelligence and answers to all network security issues, but manually reviewing the log data was not effective and was leaving their IT network at a huge risk. With a tremendous rise in data breaches across the globe, the IT department wanted to build a proactive network security system to avoid data thefts.

> "Monitoring Syslog and Eventlog data at a central place is very crucial when having a highly distributed IT network environment and EventLog Analyzer has done the job of streamlining our log management beautifully."
>
> **Network Security Administrator,**
> Indirect Taxation Authority,
> Bosnia and Herzegovina

ITA's network infrastructure included devices and systems such as routers, firewalls, programmable switches and Linux/Unix machines, which generated Syslog data. The IT team wanted to centrally manage Syslog data generated by their distributed network infrastructure in real-time. Collecting, monitoring, analyzing and archiving Syslog data without an automated approach was impossible.

Also, Indirect Taxation Authority wanted to monitor the Event Logs generated by their Windows Domain Controllers for all user activities on their network. With more than 3500 users at 80 locations throughout Bosnia and Herzegovina accessing the IT resources, it was getting very difficult to keep a track on their activities. The theft or misuse of company's assets and customer data poses a huge security threat for every organization and Indirect Taxation Authority wanted to curb Insider threat proactively with an automated solution. To overcome the insider threat challenge, Indirect Taxation Authority had to monitor and analyze on all user activity in real-time especially user logon/logoff and object access activity across their network.

"We needed to automate our log management process. Monitoring log data manually for our network security purpose is not possible when you are running a highly distributed IT network." said the Network Security Administrator, Indirect Taxation Authority, Bosnia and Herzegovina.
The Indirect Taxation Authority needed a tool that could automate log management and boost network security for their highly distributed IT environment.

Solution

The IT network security/administration team at Indirect Taxation Authority was looking for a potential solution to meet their complex log management challenges and ended up landing on ManageEngine EventLog Analyzer's website (www.eventloganalyzer.com). The team was thrilled to see that this Security Information and Event Management (SIEM) software for Log Management had a 30-day fully functional trial version. The Network security administrator immediately downloaded EventLog Analyzer and after a detailed evaluation was convinced that it was exactly what Indirect Taxation Authority needed to meet its network security and log management challenges.

EventLog Analyzer's centralized, agentless log collection was an absolute fit for Indirect Taxation Authority's distributed network environment *(Note: Optional, agent-based log collection is also supported in EventLog Analyzer)*. Collecting Syslog data from the routers, switches, firewalls, Linux machines and Event log data from Domain Controllers and other Windows-based machines was seamlessly done by EventLog Analyzer. "Monitoring Syslog and Eventlog data at a central place is very crucial when having a highly distributed IT network environment and EventLog Analyzer has done the job of streamlining our log management beautifully." says the Network Security Administrator, Indirect Taxation Authority, Bosnia and Herzegovina.

The IT network security/administration team at Indirect Taxation Authority was glad to find that EventLog Analyzer provided them with a forensic trail of all user activities that happened on their network. EventLog Analyzer's out-of-the-box user activity reports helped Indirect Taxation Authority to automatically capture user activity such as user logon, user logoff, failed logon, object access and all other activities carried out by their users in real-time. "EventLog Analyzer's user activity reports give me a clear and detailed picture of all activities that happen on my network. Tracking suspicious user activity was never so easy!" says the Network Security Administrator, Indirect Taxation Authority, Bosnia and Herzegovina.

EventLog Analyzer met all the challenges faced by Indirect Taxation Authority by monitoring network log data in real-time and providing them with complete visibility on what's happening on the network.

"EventLog Analyzer empowered our IT department with security intelligence to discover potential threats and prevent unauthorized access to confidential data." says the Network Security Administrator, Indirect Taxation Authority, Bosnia and Herzegovina.

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