A Practical Low-Cost Security Solution for Log Management and File Integrity Monitoring

Lei Chen[1], Ming Yang[2], Hayden Wimmer[3], Brittany Wilbert[4]

{lchen@georgiasouthern.edu[1], MYang8@kennesaw.edu[2], HWimmer@georgiasouthern.edu[3], BMW005@shsu.edu[4]}

Department of Information Technology, Georgia Southern University, Statesboro, Georgia, USA[1,3], Department of Information Technology, Kennesaw State University, Kennesaw, Georgia, USA[2], Google, Mountain View, California, USA[4]

Abstract. Log management and file integrity are among the most critical security controls in protecting valuable business data assets against internal and external security attacks. Despite the importance of these controls, many businesses, especially smaller ones, do not practically implement the controls due to reasons including cost and personnel. In this research, we propose a framework, utilizing low cost or free-of-cost tools, and offer guidance for efficient log management and integrity monitoring. A detailed list of relevant hardware, software, and tools as well as their corresponding costs is provided to assist businesses in strategic security planning.

Keywords: security, log management, file integrity monitoring, low-cost, forensics.

1 Introduction

A Data Breach Investigation report by Verizon indicated that a litter over half of small businesses were affected by malware and almost three quarters were affected by hacking incidents in 2019 [1]. Among the various reasons to this situation are the two critical difficulties that small businesses are facing: cost and personnel. Compared to mid-size and large-scale businesses, small businesses typically do not have sufficient funds or personnel to plan, implement, test or evaluate the security of their systems and networks which potentially leads to critical data breaches as well as system and network malfunctions detected long after they occurred [2][3][4]. Therefore, there is an acute need for developing a framework with a set of recommended hardware, software, and tools for log management and file integrity at low cost for businesses which cannot afford large-scale security solutions.

To answer the increasing demand for low-cost yet efficient security solutions for small businesses, our research proposes a framework solution meeting their needs. While security requires preventative, detective, and responsive mechanisms in multiple layers, such as firewalls, antivirus and antimalware software, and intrusion detection and prevention systems (IDS/IPS), our interest in this study focuses on the log management and file integrity. The rationale is that, despite the fact that many intrusions (appeared as changes to files and logs) can be potentially discovered via log management and file integrity checks, they still occurred in an environment protected by firewalls and other security mechanisms. Most small businesses either have not realized its importance or have not found a sound solution meeting their budget. In the

EAI MOBIMEDIA 2020, August 27-28, Harbin, People's Republic of China

DOI 10.4108/eai.27-8-2020.2294894

next few sections, a brief introduction to log management and file integrity monitoring and the corresponding standards and regulations is given [5].

2 Log Management and Requirements

In a small business, audit log data is generated by hardware, operating systems, services and applications. Log management includes the collection and inspection of such log data. Such mechanisms require monitoring audit logs and creating reports as well as analysis that can be easily reviewed by lightly trained personnel. In order to meet security standards and regulations, such as the Payment Card Industry (PCI) PCI-DSS Requirement 10.6, a formal log review structure should be in place ensuring that daily monitoring of events is performed [6].

According to HIPAA News Releases & Bulletins, every year hundreds of thousands of patients' health information was exposed due to HIPAA privacy violations [7]. In an effort to prevent and detect such data breaching, both private industry and federal authorities have established standardized processes that include log management as a core requirement. Small businesses have the responsibility to ensure that their log management procedures and operations are meeting the requirements of the latest regulations and standards which also require the capability for forensic review when necessary.

As an example, regulatory agencies and regulations such as the PCI-DSS and the SOX (Sarbanes-Oxley Act) require companies to monitor and audit log files created in their infrastructures [8][9]. In order to avoid tremendous fines and fees due to data loss, small businesses must implement sound and efficient log management and data retention. Based on the studies of regulations and industry practices, we recommend the following process for collecting log messages and establishing and documenting standard operating procedures (SOP). A framework of log management and file integrity monitoring with details of tools and costs is presented later in this paper.

Log Retention Policy requires the length of time for which logs should be kept. Depending on regulatory requirements, log retention time must be at least 30 days, with typical retention time between one to seven years. Data storage space, e.g. hard drive size allocated for logs, can be determined based on the initial storage and long-term storage. For Linux environment log collection, rsyslog is recommended, and for Windows environment tool Snare is recommended to convert Windows formatted EVT log files to Syslog, which can then be sent to central log management locations. In this way, syslog configuration can be set for all system regardless of platforms. According to PCI-DSS Requirement 10.6 [8], log messages should be reviewed on a daily basis. Such log reviewing can be done manually or automatically, with necessary alerting mechanism set in place for the latter.

3 File Integrity Monitoring (FIM) and Requirements

File integrity monitoring (FIM) is critical implementation and practice for all companies and organizations to prevent and detect unauthorized modifications to their information assets. FIM can not only detect malicious attacks from outside of the organization, but also intentional or accidental changes to data without permission due to many reasons, such as system and

software bugs and failure, human mistakes, etc. We emphasize the importance of FIM for the following reasons. Without using FIM, an organization may overlook a potential compromise that may cripple the organization leaving little or no audit trails, which are necessary for forensic investigations. Therefore, it is wiser to invest on FIM for the protection of the information assets [10][11]. Study has shown that 87% of small businesses do not have internal documented security procedures or best practices for their environment [12], where an incidence of accidental data loss due to employee's mistake is considered an enormous vulnerability in such environment. Hence a snapshot of the environment becomes critical to ensure a healthy baseline of hardware and software infrastructure in case of incidence.

Similar to log management, regulatory agencies and regulations also require companies and organizations to include file integrity monitoring within their environment [8]. Small businesses have to provide documentation as well as implement the technical requirements necessary to implement FIM within the environment. Following these regulations and industry practices, we suggest the following FIM configuration process, which should be included in the established and documented standard SOP of an organization.

FIM tool needs to be configured to not only protect the environment but also guard FIM itself from potential tampering. The fingerprint, a file used for verifying the integrity of data compared to its earlier version utilizing cryptographic hash functions, such as the Secure Hash Algorithm 2 (SHA-2), must be backed up and stored in a secure manner. Upon the completion of FIM tools in the environment, reviews of alerts from these tools, such as the Open Source Tripwire, need to be closely monitored. If a red flag is raised, further in-depth review should be performed and escalation to relevant parties may be necessary. At any event of adding a new patch of major system update, the fingerprint must be updated to ensure the review of system and network activities is accurate based on the current state of the environment.

4 Proposed Framework for Log Management and FIM

In this section, we first introduce a number of tools for our proposed log management and file integrity monitoring framework. These tools have been tested and are used in daily practice. We also include a section of our tool analysis and list the cost for small businesses to implement the framework.

4.1 Tools

In the selection of tools, considering minimizing the cost to small businesses or businesses with a tight financial budget, several open source or free tools are identified and reviewed. These tools combined will provide sufficient functionality for log management and FIM. Our recommended tools also avoid major licenses for use in a small business environment. Some of these tools have equivalent enterprise versions with a certain cost. This will happen when a small business has expanded to a larger size and their employment number has exceeded the allowed maximal number for the free version of the tools. However, most businesses in such scale will more likely have a better financial situation and tend to be more willing to invest in the security of their systems and networks. In our proposed framework, six software tools and services are used to create a system for log management and FIM.

1) Rsyslog

Syslog is the default Linux log manager. Rsyslog extended syslog by adding features such as listening the TCP traffic, and therefore supports both local and remote log management. It has a robust configuration system that gives very fine-grained level of control over what to collect, how to collect, where to store the log files, as well as how logs are configured for future analysis.

2) Snare

Snare has the capabilities of filtering, reviewing, and sending Windows proprietary event logs. One extra bonus feature of Snare however is it can configure/convert Windows log messages into Linux syslog format and send them to a (remote) centralized location for log management. In our daily practice, we use Snare as a compliment to rsyslog for Windows platforms.

3) Logstash

The open source log filtering tool Logstash has a simple interface for easy and quick log management, which makes it suitable for small businesses. Logstash can be used along with other tools such as Elasticsearch and Kibana (later in this section) for analyzing and filtering various types of log messages. Logstash also allows to use Bash or Perl scripts to integrate plug-ins for enhancing alerts and notifications. Another advantage of Logstash is that it works on multiple Linux distributions, including Ubuntu.

4) Elasticsearch

Elasticsearch is used for log collection and storing logs in server database. A highly valued feature of Elasticsearch is that it works seamlessly with Logstash to store filtered log messages at a central location, and it also works perfectly with programs such as Kibana for people who prefer GUI log management interface. Elasticsearch is available in both a demonstration level and business software packet for various Linux distributions.

5) OSSEC

OSSEC is a multi-purpose security management tool that is capable of file integrity monitoring, reporting system changes, and incident remediation, such as remote firewall changes and blocks. With both an open source and enterprise versions, OSSEC is frequently updated with new versions. OSSEC supports agent on Windows platform and both server and agent for Debian and Red Hat Linux. In the proposed framework, OSSEC is only used for file integrity monitoring purpose.

6) Kibana

Kibana allows for visualization of audit log events in the environment for efficient and easy log management, including providing clear and concise event logs understandable by lightly trained personnel. Since Kibana works well with Elasticsearch and Logstash, it is recommended in our proposed framework. Plug-ins are available for integrating Kibana into Elasticsearch and Logstash, so the installation and configuration becomes simple and straightforward.

4.2 Software Configuration

The software configurations are very important in the proposed framework for a system with different tools working seamlessly. As an example, discussions below are based on an Ubuntu Linux Server 18.04 LTS functioning as the central log management server.

Rsyslog on the server was configured to allow incoming traffic using UDP port 514. A template of log configuration script was created as shown in Figure 1. Snare was configured to allow IIS (Internet Information Service) log messages to be viewed. Logstash needs to be

configured so that data from Rsyslog, OSSEC, and Snare can be filtered and then properly recorded. A portion of such configuration script is shown in Figure 2 as an example. This filter allows for syslog files that are in rsyslog format to be filtered through Logstash.

```
###### 1. Install and configure rsyslog server
### Update rsyslog file (assuming file is in default location
/etc/rsyslog.conf and has not been modified)
sed -i 's/\#\$ModLoad imdp/\$ModLoad imdp/g' /etc/rsyslog.conf

sed -i 's/^\#\$UDPServerRun 514/\$UDPServerRun 514/g' /etc/rsyslog.conf

sh -c 'echo "\$template(name=\"TmplAuth\" type=\"string\"" >>
/etc/rsyslog.conf'

sh -c 'echo "    string=\"/var/log/%HOSTNAME%/%PROGRAMNAME%.log\"" >>
/etc/rsyslog.conf'

sh -c 'echo "\)" >> /etc/rsyslog.conf'

sh -c 'echo "\$template(name=\"forwardFormat\" type=\"string\"" >>
/etc/syslog.conf'

sh -c 'echo "    string=\"<%PRI%>%TIMESTAMP\:\:\:date-rfc3339 %HOSTNAME%
%syslogtag\:1\:32\:%%msg\:\:\:sp-if-no-sp%%msg%\"" >> /etc/syslog.conf'

sh -c 'echo "\)" >> /etc/rsyslog.conf'
```

Fig. 1. A template of log configuration script for Rsyslog.

```
filter {
  if [type] == "syslog" {
    grok {
      match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp}
%{SYSLOGHOST:syslog_hostname} %{DATA:syslog_program}(?:
\[%{POSINT:syslog_pid}\])?: %{GREEDYDATA:syslog_message}" }

      add_field => [ "received_at", "%{@timestamp}" ]
      add_field => [ "received_from", "%{host}" ]
    }
    syslog_pri { }
    date {
      match => [ "syslog_timestamp", "MMM  d HH:mm:ss", "MMM dd
HH:mm:ss" ]

    }
  }
```

Fig. 2. A portion of example Logstash configuration script.

Other configurations of these tools are quite straightforward with just one note to be addressed. The OpenSSL certificates must be installed on log management server and the Kibana server in order to make Kibana work.

4.3 Cost of Implementation

The cost of implementation consists of hardware, software, and personnel. The estimated cost addressed below is for typical scenarios in a small business environment (e.g. total employee number less than 100) [13], assuming the existence of common infrastructure that a small business would have, such as broadband internet access, properly configured routers, switches and local area networks (LANs). The details of unit costs and total costs for the hardware and software of the proposed framework can be found in Table 1.

Table 1. Approximate Hardware/software Cost.

Hardware / Software	Instances Implemented	Unit Cost	Total Cost
Desktop computer	1	$900.00	$900.00
Snare	1	$0.00	$0.00
Rsyslog	4	$0.00	$0.00
Logstash	1	$0.00	$0.00
Elasticsearch	1	$0.00	$0.00
Kibana	1	$0.00	$0.00
OSSEC	5	$0.00	$0.00
Windows 10 Pro	1	$199.99	$199.99
Ubuntu Servers (VMs)	4	$0.00	$0.00
1 TB Hard drive	2	$70.00	$140.00
Total			**$1,239.99**

The estimated personnel cost is shown in Table 2. Based on this information, if a single employee is employed to work on these tasks with the installation, configuration, and maintenance of two Ubuntu servers, two Ubuntu Desktops, and one Windows workstation allow with the daily review of the activity that results, it would cost approximately $13,417.83 at an hourly pay rate of $30.21. However, a larger infrastructure would cause an increase in this cost, particularly if there are increases in the number of systems in the environment, log messages that require review and the number of incidents that occur. This also does not include any additional roles personnel may be fulfilling.

Table 2. Approximate Annual Personnel Cost.

Tasks	Hours Per Week	Hourly Cost Per Week ($)	Total Cost per year ($)
Hardware installation (Single Cost)	2	61.41	61.41
Software installation – Windows 10: 1 instance (Single Cost)	1.5	46.82	46.82
Software installation – Virtualbox (Single Cost)	4	122.82	122.82
Software configuration – Virtualbox (Single Cost)	0.5	15.11	15.11
Virtualbox configuration – Ubuntu servers – 2 workstations and 2 servers (Single Cost)	6	187.28	187.28
RSyslog configuration (Single Cost)	2	$30.21	61.41
Snare Configuration (Single Cost)	2	$30.21	61.41
Logstash configuration (Single Cost)	2	$30.21	61.41
OSSEC Configuration – Agent: 4 instances	1.5	46.82	46.82
OSSEC Configuration – Server: 1 instance	0.5	15.11	15.11
Elasticstash configuration (Single Cost)	2	$30.21	61.41
Kibana Configuration (Single Cost)	2	$30.21	61.41
Script Creation and Testing (Single Cost)	25	755.25	755.25
Maintenance and Updates (estimate per week)	1	30.21	1570.92
Daily Log Review (estimate per week)	5	151.05	7854.6
Incident Response (estimate per week)	1.5	46.82	2434.64
Totals	***Total Hours: 58.5***	***Total Individual Cost (Per Week): $1,629.75***	***Estimated total cost/year: $13,417.83***

5 Conclusion and Future Work

Implementation of a security framework within a small business is a vital component to provide protection of the intellectual property of small organizations. Although small businesses may not hire as many employees as large corporations, the number of small businesses alone with infrastructure in risk as a result of non-existent or insufficient security may allow for these businesses to be exploited without recourse and open the potential for ransomware as well as other attacks.

Furthermore, although this work is specifically focused on small businesses with relatively tight budgets, there are many other public and private industries which may organize portions of their businesses like a small business for periods of time. Implementing some of the framework requirements may allow for these departmental structures to be transitions to more formal processes and procedures within the organization.

Small businesses have unique obstacles that are not faced by larger or more established organizations. Because they are more likely to be compromised by malicious users, the cost of deploying solutions to mitigate compromise can be unaffordable, and individuals that are tasked to manage these solutions may not have the time or resources available to effectively monitor and protect against incidents. Due to this, small businesses must find alternate solutions that will fit their environment and existing infrastructure.

The Small Business Framework with the proposed Log Management and File Integrity Monitoring is to provide small businesses starting resources that can be used to monitor their fragile environments holistically while they are growing their business. The ultimate goal of the framework is to allow the opportunity for guidance to be provided to these businesses that can be expanded on in the future. Although there are other solutions which may be used to obtain a similar result, applying some of the techniques discussed in this paper can allow small business organizations to better prepare for security events that may occur within their environment.

Cloud computing allows for small businesses and other enterprises to leverage public and private infrastructure in order to potentially lessen the cost of infrastructure and security requirements for the organization. Integrating cloud log management and file integrity monitoring into the security framework would be the next work. While integration of cloud computing is important to provide a discussion to small businesses, the importance of proper contracts and Service Level Requirements (SLA) becomes a higher necessity. Without strict contracts a cloud computing organization could pose a greater risk to the security data of the organization than the organization's technological structure. It must also be considered how the cloud computing structure, regardless of if it is created by a small business itself or a third party, is properly segmented and protected from threats.

References

[1] Verizon Enterprises, "2019 Data Breach Investigations Report," Verizon Enterprises, 2019. [Online]. Available: https://enterprise.verizon.com/ resources/reports/dbir/. [Accessed February 20, 2020].

[2] Ready.org, "Business Impact Analysis," Ready. 11 December 2015. [Online]. Available: http://www.ready.gov/business-impact-analysis. [Accessed February 24, 2020].

[3] Microsoft, "Step 1 - Identifying Risks in Operations," Microsoft Corporation, 19 April 2010. [Online]. Available: http://technet. microsoft.com/en-us/library/cc535338.aspx. [Accessed February 25, 2020].

[4] Serhiy Kozlov, "Disaster Recovery Plan: How to Ensure Business Continuity," 6 February 2019. [Online]. Available: https://www. business2community.com/business-innovation/disaster-recovery-plan-how-to-ensure-business-continuity-02166281. [Accessed February 25, 2020].

[5] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations," 2013. [Online]. Available: http://nvlpubs.nist.gov/ nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.[Accessed February 21, 2020].

[6] U.S. Department of Health and Human Services, “Summary of the HIPAA Privacy Rule,” 2014. [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/. [Accessed February 21, 2020].
[7] HIPAA News Releases & Bulletins, 2020. [Online]. Available: https://www.hhs.gov/hipaa/ newsroom/index.html. [Accessed February 22, 2020].
[8] Asim Mehmood, “An Introduction to PCI DSS,” 23 March 2018. [Online]. Available: https://www.cryptomathic.com/news-events/blog/ an-introduction-to-pci-dss. [Accessed February 23, 2020].
[9] Sarbanes Oxley 101, “Sarbanes Oxley Aduit Requirements,” 27 February 2020. [Online]. Available: https://www.sarbanes-oxley-101. com/sarbanes-oxley-audits.htm. [Accessed February 27, 2020].
[10] U.S. Security and Exchange Commission, “Sarbanes-Oxley Section 404: A Guide for Small Businesses,” U.S. Security and Exchange Commission, 22 January 2008. [Online]. Available: https://www.sec. gov/info/smallbus/404guide/intro.shtml. [Accessed February 22, 2020].
[11] Microsoft, “Risk Management Process Overview,” Microsoft, 19 April 2010. [Online]. Available: http://technet.microsoft.com/en-us/library/ cc535304.aspx. [Accessed February 23, 2020].
[12] J. M. Johansson and R. Grimes, “The Great Debate: Security by Obscurity,” Microsoft Corporation, June 2008. [Online]. Available: http://technet.microsoft.com/en-us/magazine/2008.06. obscurity.aspx. [Accessed February 22, 2020].
[13] The U.S. Small Business Administration, “Table of Size Standards,” 2019. [Online]. Available: https://www.sba.gov/document/support--table-size-standards. [Accessed February 21, 2020].