Security - How to Measure Compliance
MIPRO 2008

O. Mirković
Information Security Coordinator
Ericsson Nikola Tesla
Krapinska 45, Zagreb, HT-10002, Croatia
Phone: +385 (91) 365 3287 Fax: +385 (91) 365 3219 E-mail: orlan.mirkovic@ericsson.com

Abstract - Information security requirements are growing in complexity and importance. Furthermore auditing requires compliance with predefined standards like GLBA, HIPAA, PCI DSS, SOX, to be met and measured. This article explains how to implement security measurements to be compliant with above mentioned standards.

I. INTRODUCTION

Not just in security but in industry in general, quality of service and quality assurance drives the market to continuously measure the risk and more important, to react on preset thresholds.

Furthermore companies around the world competing for the segment of the market are facing yet another challenge: alignment and compliance with security standards. External auditors are coming once or twice a year in the company asking more and more controls to be fulfilled and they are searching for evidence.

Now, it would be easy with upper management support (read: money and time supply in abundance), but budget is limited and standards are too big, interrelated, and very often provide us with a guidance only. Tools are expensive, and very often provide us with enough functionality during the design and definition stage, but they are very often rigid when we want to apply change coming from the change management process and/or require significant future investment in time and money. Further ITIL process requires SLA review once or twice yearly so it would be a significant portion of time spent on just aligning operations with updated SLAs.

The last motivation is a level of abstraction lower. The company I work for has very disparate market coverage: large contract with health industry, consultancy with various government offices, financial institutions, and companies of various strategic and national importance. All of them require alignment with different set of standards. Having a process to be able to build a project that will meet such a broad coverage of standards is a huge comparative advantage at the market. And behind the scene is a preparation for future to start to create a product.

So the question to be answered is: how to align our measurements with standards mentioned in the summary of this article, and what metrics to use to keep the auditor happy on one hand, and SLAs on the other.

II. SCOPE AND DEFINITIONS

Let us just define what each standard requires regarding the functionality.

A. GLBA Compliance Audit Reports

Section 501 of the Gramm-Leach-Bliley Act (GLBA) [1] documents specific regulations required for financial institutions to protect "non-public personal information".

As part of the GLBA requirements, it is necessary that a security management process exists in order to protect against attempted or successful unauthorized access, use, disclosure, modification, or interference of customer records. In other words being able to monitor report and alert on attempted or successful access to systems and applications that contain sensitive customer information.

The types of reports to be provided for GLBA Compliancy Audits are as follows:

1) User Logon report: GLBA Compliance requirements clearly state that user accesses to the system be recorded and monitored for possible abuse. Remember, this intent is not just to catch hackers but also to document the accesses to medical details by legitimate users. In most cases, the very fact that the access is recorded is deterrent enough for malicious activity, much like the presence of a surveillance camera in a parking lot.

2) User Logoff report: Defines a user activity together with the User Logon report.

3) Logon Failure report: The security logon feature includes logging all unsuccessful login attempts. The user name, date and time are included in this report.

4) Audit Logs Access report: GLBA requirements (review and audit access logs) calls for procedures to regularly review records of information system activity such as audit logs.

5) Security Log Archiving Utility: Periodically, the system administrator will be able to back up encrypted copies of the log data and restart the logs.

B. HIPAA Compliance Reports

The Health Insurance Portability and Accountability (HIPAA) [2] regulation impacts those in healthcare that exchange patient information electronically. HIPAA regulations were established to protect the integrity and security of health information, including protecting against unauthorized use or disclosure of the information. HIPAA states that a security management process must exist in order to protect against "attempted or successful unauthorized access, use, disclosure, modification, or interference with system operations". In other words being able to monitor report and alert on attempted or successful access to systems and applications that contain sensitive patient information.

The types of reports for HIPAA Audits are as follows:

1) User Logon report: HIPAA requirements (164.308 (a)(5) - log-in/log-out monitoring) clearly state that user accesses to the system be recorded and monitored for possible abuse.

2) User Logoff report: Defines a user activity together with the User Logon report.

3) Logon Failure report: Includes logging all unsuccessful login attempts.

4) Audit Logs Access report: HIPAA requirements calls for procedures to regularly review records of information system activity such as audit logs.

5) Object Access report: Identify when a given object (File, Directory, etc.) is accessed, the type of access (e.g. read, write, delete) and whether or not access was successful/failed, and who performed the action.

6) System Events report: Identifies local system processes such as system startup and shutdown and changes to the system time or audit log.

7) Host Session Status report: Indicates that someone reconnected to a disconnected terminal server session. (This is only generated on a machine with terminal services running).

8) Successful User Account Validation report: Identifies successful user account logon events, which are generated when a domain user account is authenticated on a domain controller.

9) UnSuccessful User Account Validation report: Identifies unsuccessful user account logon events, which are generated when a domain user account is authenticated on a domain controller.

10) Security Log Archiving Utility: Periodically, the system administrator will be able to back up encrypted copies of the log data and restart the logs.

C. PCI-DSS Compliance Reports

Payment Card Industry Data Security Standard (PCI-DSS) Requirement 10, [6] which enables payment service providers and merchants to track and report on all access to their network resources and cardholder data through system activity logs. The presence of logs in networked environment allows thorough forensic analysis when something does go wrong. Without system activity logs it would be difficult to determine the cause of a compromise.

The types of reports to be provided for PCI audits are as follows:

1) User Logon report: PCI-DSS requirements 10.2.1 all individual user accesses to the system be recorded and monitored for possible abuse. In most cases, the very fact that the access is recorded is deterrent enough for malicious activity, much like the presence of a surveillance camera.

2) User Logoff report: Defines a user activity together with the User Logon report.

3) Logon Failure report: PCI-DSS requirements 10.2.4 - Includes logging all unsuccessful login attempts.

4) Audit Logs Access report: PCI-DSS requirements 10.2.6 - regularly review records of information system activity such as audit logs.

5) Object Access report: PCI-DSS requirements 10.2.7 - Identify when a given object (File, Directory, etc.) is accessed, the type of access (e.g. read, write, delete) and whether or not access was successful/failed, and who performed the action.

6) Track Audit Policy Changes report: PCI-DSS requirements 10.2.3 - Access to all audit trails, lets organizations to comply with internal controls by tracking the event logs for any changes in the security audit policy.

7) Track Individual User Action report: PCI-DSS requirements 10.1, 10.2.2 - lets organizations to comply with internal controls by auditing access to system components to each individual user and tracking the actions performed by any individual.

D. SOX Compliance Reports

In *Section 404* - Management Assessment of Internal Controls and *Section 302* - Corporate Responsibility for Financial Reports of the Sarbox or SOX act, lays the foundation on how IT can aid SOX compliance.

The types of reports to be provided for SOX audits are as follows:

1) User Logon report: SOX requirements (Sec 302 (a)(4)(C) and (D) - log-in/log-out monitoring) [3] clearly state that user accesses to the system be recorded and monitored for possible abuse.

2) User Logoff report: SOX requirements (Sec 302 (a)(4)(C) and (D) - Defines a user activity together with the User Logon report.

3) Logon Failure report: Includes logging all unsuccessful login attempts.

4) Audit Logs Access report: SOX requirements (Sec 302 (a)(4)(C) and (D) - review and audit access logs) calls for procedures to regularly review records of information system activity such as audit logs.

5) Object Access report: Identify when a given object (File, Directory, etc.) is accessed, the type of access (e.g. read, write, delete) and whether or not access was successful/failed, and who performed the action.

6) System Events report: Identifies local system processes such as system startup and shutdown and changes to the system time or audit log.

7) Host Session Status report: Indicates that someone reconnected to a disconnected terminal server session. (This is only generated on a machine with terminal services running).

8) Security Log Archiving Utility: Periodically, the system administrator will be able to back up encrypted copies of the log data and restart the logs.

9) Track Account Management Changes: Significant changes in the internal controls sec 302 (a)(6). Changes in the security configuration settings such as adding or removing a user account to an administrative group. These changes can be tracked by analyzing event logs.

10) Track User Group Changes: Tracking event logs for changes in the security configuration settings such as adding or removing a global or local group, adding or removing members from a global or local group, etc..

11) Track Audit Policy Changes: Corporations must comply with internal controls sec 302 (a)(5) by tracking the event logs for any changes in the security audit policy.

12) Successful User Account Validation Report: Identifies successful user account logon events, which are generated when a domain user account is authenticated on a domain controller.

13) UnSuccessful User Account Validation Report: Identifies unsuccessful user account logon events, which are generated when a domain user account is authenticated on a domain controller.

14) Track Individual User Actions Report: Corporations must comply with internal controls sec 302 (a)(5) by auditing user activity.

15) Track Application Access: Corporations must comply with internal controls sec 302 (a)(5) by tracking application process.

That would conclude our listing of main security standards.

III. CONSOLIDATION

In this perspective the above mentioned controls were to be grouped and consolidated.

Second step is to map the existing logging mechanisms in IT to the requirements from the standard.

A. Consolidation

Let's just sort the controls, sort them and see what (number) of controls we have to comply with to cover ALL standards:

TABLE I
CONSOLIDATION OF CONTROLS
OK if the control is applicable for the respective standard

Controls	**GLBA**	**HIPAA**	**PCI-DSS**	***SOX***
User Logon Report	*OK*	*OK*	*OK*	*OK*
User Logoff Report	*OK*	*OK*	*OK*	*OK*
Logon Failure Report	*OK*	*OK*	*OK*	*OK*
Audit Logs Access Report	*OK*	*OK*	*OK*	*OK*
Object Access Report		*OK*	*OK*	*OK*
System Events Report		*OK*		*OK*
Host Session Status Report		*OK*		*OK*
Security Log Archiving Utility	*OK*	*OK*		*OK*
Track Account Management Changes				*OK*
Track User Group Changes				*OK*
Track Audit Policy Changes			*OK*	*OK*
:Successful User Account Validation Report		*OK*		*OK*
UnSuccessful User Account Validation Report		*OK*		*OK*
Track Individual User Actions Report			*OK*	*OK*
Track Application Access				*OK*

With this crude analysis we can argue everybody that if we cover SOX, we cover them all.

A. Mapping to existing logging mechanisms in IT

Immediately two mechanisms are coming into our mind:

1) Logs: Syslog (or equivalent) in Unix world, or Event log in Windows world. This mechanism covers all tracking logging on and off, and changes. Audit exists as well but on application level.

2) Group Policies: Unfortunately Unix world does not have the same concept to it. Domain Controller with Active Directory provide us with setting to turn on the Audits for nearly anything we need from the TABLE I. Unfortunately it is not turned on by default.

IV. SOLUTION

A. Architecture

So, now we have defined and clarify what do we need to comply with the standards:

1) events,

2) traffic,

3) logs and

4) group policies changes.

This conclusion helped us tremendously with narrowing down the search for tools.

Our final "compliance" tool now consists of:

1) Firewall analyser [4],

2) Event Log Analyser (both Unix and Windows),

3) An integration tool to gather audit logs from different technology platforms [5],

4) A reporting tool with fine granularity of roles, so virtually everybody has some level (executive, technical, read-only, domain, decentralized configuration…) of management and

5) A documented procedure how to create the report by using the data gathering tools.

NOTE: Brands are not mentioned due to educational character of the article.

B. Functional Requirements

The most important part and the one that brings the business value to it is easy and managed customization of the system. Customization enables two crucial features:

1) Shorten the period of required report or alert from the need to the implementation and

2) "Post mortem" and trend reporting from the data stored in longer period of time.

One example would be following the history of evidence after the system alerts you a particular user tried to unsuccessfully logon on a particular system. That incident can be followed by creating a new report that follows that particular user and it IP address.

The next case is creating alert, correlation and policy change (!!!) when unauthorized wireless access point is noticed through previously uncorrelated alerts and after running the newly created correlation through the history logs finding the source of it.

IV. CONCLUSION

What benefits came out of this kind of approach to implementation of the security standard.

1) Last two audits were a pain: Running around for documents, trying to find an example of login failure, tracking of a particular application, etc. This year I was answering on auditor questions in a matter of seconds, and basically without any outdated documentation. Everything was presented to the auditor through the above mentioned tools interactively.

2) Security actions are not reactive any more, but we came to the point where we can actually plan the future actions.

3) Uses standard data that every IT department can easily provide,

4) Makes auditors happy,

5) Provides the management with exact figures.

Also once when the whole exercise has been completed, with near real-time reporting available, the need for alerting came up into focus. This is obviously the next step to be implemented. Building and grouping alerts are very easy to grasp at the surface, but it requires a serious evolution in changing of the procedures in the corporate environment.

REFERENCES

[1] Tufts University, “Gramm-Leach-Bliley Act: Information Security Program”, *http://whitepapers.techrepublic.com.com/,* 2004.

[2] Gilbreath, Allan, "HIPAA Security Technology Compliance", McGraw-Hill Osborne Media, ISBN 007223198X, 2004

[3] Stewart M. Landefeld, Andrew B. Moore, Jens M. Fischer, " The Public Company Handbook: A Corporate Governance and Disclosure Guide for Directors and Executives", SecuritiesConnect™, 2006

[4] Oracle, “System Monitoring Plug-in for Juniper Netscreen Firewall”, *http://www.oracle.com/technology/ob,* 2008.

[5] Argent, “Argent Enterprise View”, *http://www.argent.com/,* 2007.

[6] Argent White Paper, "Argent Compliance Series: PCI", *http://www.argent. com/,* 2007.