Analysis of Role of SDLC in Cloud Security based on various incidents

Nirav R. Madhani
Computer Science and Engineering
Institute of Technology, Nirma University
Ahmedabad, India
18bce135@nirmauni.ac.in

Niketkumar N. Kothari
Computer Science and Engineering
Institute of Technology, Nirma University
Ahmedabad, India
18bce134@nirmauni.ac.in

ABSTRACT

A recent NEWS revealed that the Ransomware attack on a hospital in Europe could be held responsible for patients' death. It is the first recorded death in human history due to a cyber attack. Investigation revealed that potential security loopholes had been identified and reported earlier but the team ignored this warning; which later had severe consequences. This incident has encouraged us to carry out detailed research and analysis in this area and how one's approach at early stages of SDLC plays roles in various aspects. The essence of this paper is the study of Security issues and the importance of security in SDLC Models. Development area as we differentiate in the traditional SDLC Security issues in virtualized SDLC security Scenarios like a cloud. Here, we discussed the role of the team in the feasibility and planning phases of the analysis. This study deals with access control, risk assessment and security Supervision.

1. INTRODUCTION

In our analysis, we explored the roles / responsibilities of developing members of the team and computing efforts in various SDLC phases to figure out the places to add protection Implementation. The central requirement of everything is security.

Software providers need the security of software Infrastructures, as well as trust preservation in computing.

In order to accomplish this, suppliers must follow a strict method for designing software that focuses on security so that plan, coding, documentation and protection vulnerabilities other stages can be reduced, defined and eliminated as in the development life cycle, as early as possible. And for security purposes, a team of skilled people must always be there for Frequent interactions during the creation of applications and evolution. The same category is expected to have a final protection examination, FSR, until release of the software.

2. BACKGROUND

In 2010, Microsoft experienced a breach within its Business Productivity Online Suite that was traced back to a configuration problem. The issue allowed non-authorized users in their offline address books to access employee contact info. It affected only a small number of users, but it is worth noting.

More than 68 million DropBox accounts were hacked in 2012. Stolen credentials reportedly made their way to a dark web marketplace. At the time, the price for the credentials was in bitcoins – roughly equal to $1,141. Dropbox responded by requesting a site-wide password reset from the user base.

In May 2016, hackers stole and posted for sale on the dark web an estimated 167 million LinkedIn email addresses and passwords. In Response to that, LinkedIn implemented two-way authentication, an optional feature that makes you enter a pin code on your mobile device.

3. SECURITY IN VARIOUS STAGES OF SDLC

A. Phase Requirements

A member of the software security team / group accompanies the remaining members of the phase to make recommendations related to security and specially advised as follows:-

1. Security Milestones
2. Criteria for exit

These advice are based on the size of the project, the risks, and other factors. The member may be referred to as "Security Advisor." The Member shall monitor the security element in such a way that it does not face problems in later phases. This phase is the basis for how security is integrated in the next phases and

Identification of key safety objectives.

B. Design Phase

This stage determines the software's overall structure.
The concept of security architecture and design, therefore, guidelines are also included in the procedure. Along with this, Identification of the critical elements, the protection of which is of utmost importance. Principles of architecture implemented includes:

1. Least Privilege: Define those who should be granted a subject which requires privileges to complete its mission. The inspection should be practical and not identity-based. The Rights are inserted as necessary and later discarded.
2. Fail-Safe Defaults: Defaults to refuse access by default behaviour.And if the action fails, the device is as stable as when the action fails.
3. Mechanism 's economy: Keep things as simple as possible, In other words, the KISS Theory is extended where it implies that fewer can go wrong and when mistakes arise, they are easier to comprehend and repair.
4. Total Mediation: Each must be supervised Access is generally performed once, on the first action, not on the first action. After that, controlled, but if permissions alter afterwards, one unauthorized access can be obtained.
5. Open Design: Protection should not be based on the confidentiality of the plan or execution, but it shall not, be misunderstood to mean that there should be a public source code, It is "Protection by obscurity" instead, but it does not do so information such as passwords or cryptographic data is applicable to keys and so on.
6. Privilege Separation: To distinguish privilege, it requires several conditions granted right, such as division of duty and in depth protection.
7. Least Common Mechanism: There should not be mechanisms through which data can flow via a shared channel. Isolation using sandboxes and virtual machines can be done.
8. Psychological Acceptability: Mechanisms for defence should not add to the complexity of resource access. There 's got to be simple to install, customise, use, etc.

C. Development / Implementation Phase

A number of measures have been taken to control security flaws in this Phase so that the release of the final version for customers is as follows: It's better to provide special attention to the developers so that the incorrect code does not lead to high priority threats. The application of coding and testing standards therefore helps prevent security flaws. Furthermore, the application of security Tools such as "Fuzzing" that delivers structured but invalid Inputs are used to detect errors. Static analysis tools can also be detected Faults like buffer overrun, integer overrun, etc. Reviews of Code include both manual and automated code review. When automated, including error detection tools, the manual implies trained developers to monitor the accuracy of the code.

E. Deployment & Maintenance Phase
At this stage, the software must be secure enough to be ready for delivery to customers. A final security review is being conducted at this stage. In FSR, the ability of the software and the vulnerability response is monitored, along with penetration testing. The result is an overall picture of the security position of the software.

IV. SECURITY IN SDLC OVER CLOUD

The concept of the lifecycle development of software for a project varies according to many factors, including type, size and time. Majority of times,in combination with cloud computing, SDLC is more risk-prone. To work upon the concept of Merging SDLC with cloud, this paper analyzes the cloud feasibility study phase and the identification of safety and risk issues of SDLC based cloud. We are designing a secure web application process Development.

This secure process can be defined as a set Design , development, testing activities, Setting up, maintaining, and delivering a secure solution. Activities may not necessarily be sequential; they may be sequential, Can be simultaneous or iterative. We're analyzing the need for security in every Web Engineering Activity Module, as follows:

1. The problem formulation (Problem Analysis),
2. Planning module.(Feasibility Study)
3. Analysis module of requirements(Analysis of Requirement)
4. Design of architectural, navigational, and interfacesModule (Module for design)
5. In the Module for System Implementation (Development Modulus)
6. Testing and integration in the Application Unit and Management of configurations (Testing Module)
7. In quality control and mechanisms of maintenance. (Maintenance Module).

V. SECURE WEB APPLICATION DEVELOPMENT LIFE CYCLE(SWADLC)

We address and examine security issues after the debate and study.Planned to upgrade SDLC for security implementation in

Virtualized systems such as cloud computing varying scenarios for service growth. We proposed improvements to
SDLC in terms of main points being pursued as per intermediate Stages-

In requirement analysis and feasibility study

To ensure the security of virtualized resources , it is important as we use all web tools for application purposes, and non-physical development of cloud computing.

In design and development

We are processing tasks over virtualized resources via the internet so we have to configure secure data communication over a virtualized network and need to maintain a secure connection between developer’s machine and virtual machine.

In testing and configuration management

We have to be careful about individual and group testing.We have two in this module
1) Developer Side 2) Client Side

If we do developer side testing, it can be a test
on
1) Computer of the developer as local,
2) In a cloud setting as a multinational virtual machine.

I. If we test it on the developer 's screen, then it will be safer than a virtualized machine.
II. If we're checking on the client side, then virtualized checking the computer would be better than research on the client side.

We may claim protection in testing from the above two claims.
A lot of focus is needed at the time of the customer side module. Since we have two security modules to treat between the cloud and the creator, one and the other in between a cloud and a customer. Both of these security modules are very important,
In execution,
We will have to take care of the deployment and installation of this module.

In maintenance and Feedback module

Our key aim is to get input from customers and we still have to be careful about applying it to boost QoS. Process of maintenance for all customer requests after using the web application that was created. This module 's job is to feedback on any lifecycle module for Application efficiency enhancement. For this purpose, this module Deals with and improves the application of the above given model. Again it has to be careful about security issues because lots of intruders try at this point to disturb module design and codes by providing wrong feedback.

A. Security Monitoring in SWADLC

As we deal with protection in the creation of software,We have to concentrate on each lifecycle (as a process) and independently of each module, because of any protection module. The specifications are distinct from each other. We need to describe certain protection tracking points according to lifecycle patterns. Security control, as we operate over SDLC, Points are used in between SDLC modules to search protection of the previous performance of the module and protection verification over For the next module, input via a study and evaluation of current process models and guidelines, safe-secure activities, the production of applications has been graded as follows—

B. Common Module Security Activities(CMSA)

We have classified operational activities that are common to all The Modules Engineering Activities (EA): Includes engineering activities:
Activities needed to design a secure security solution Elicitation and definition requirements for infrastructure Practicability.
Assurance Activities (AA): Assurance activities include assurance activities like verification, validation as validation of the problem, expert review In order to make an informed decision on the feasibility of creating Application services in various infrastructures of the cloud.
Activities of Management(MA): These are further classified as follows—

i. MA-OA (Organizational Activities)

Organizational activities take care of organizational policies, the establishment of organizational roles, and other web security-supporting organizational activities in Environment Virtualized. Activities in project management, project planning and safe resource tracking include Process of allocation in various cloud infrastructures and usage. Such virtualized resources ensure the security of the Security assurance, engineering, and risk identification, where activities are scheduled, managed, and monitored.

ii. Activities for Risk Identification(MA-RIA)

The most important risk is to identify and manage security risks. Significant operations in a secure application development on the new risk of attacks, cloud environments are growing with rapid growth. It is the driver for successive operations such as security engineering operations, the project management activities and activities relating to security assurance.

VI. CONCLUSION

Subsequent to security and risk-related analysis
In the cloud environment of SDLC, we have now looked at Secure Web Application Implementation Part for Life Cycle development of public and private clouds. In the life cycle, insert and insert deliverables (information) that are designed to promote decision management as "Move / not move" as moving choices to jump from one stage to the next stage. This review will provide a generalization of the process involved which can be implemented during SDLC for better security on cloud.

Sources

1. R. Kumar, S. K. Pandey, S. I. Ahson, “Security in Coding Phase of SDLC” Department of Computer Science Jamia Millia Islamia, New Delhi- 110025, INDIA

2. G. McGraw, “Building Secure Software: A Difficult But Critical Step in Protecting Your Business,” Cigital, White Paper, available at: http://www.cigital.com/whitepapers/

3. L. M. Vaquero, L. Rodero-Merino, J. Caceres and M. Lindner, “A break in the clouds: towards a cloud definition”, SIGCOMM Computer Communication Review, vol.39, pp. 50-55, December2008.

4. Raj, Gaurav & Singh, Dheerendra & Bansal, Abhay. (2014). Analysis for security implementation in SDLC. Proceedings of the 5th International Conference on Confluence 2014: The Next Generation Information Technology Summit. 221-226. 10.1109/CONFLUENCE.2014.6949376.