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 purpose of this paper is to talk about security and cloud security problems in SDLC models. Development field as we see in SDLC security situations in the typical SDLC security problems like a cloud. In the preparation and the feasibility phase of the analysis we will explore the position of the team. This research includes risk evaluation, access control and compliance monitoring.

1. INTRODUCTION

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

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.

In 2012, the DropBox accounts were hacked to more than 68 million. Robbed credentials have gone to a dark web marketplace allegedly. The credentials price at the time was around $1,141 in Bitcoins. Dropbox responded by asking the user base to reset the sitewide password.
Hackers robbed 167 million LinkedIn email and passwords and placed them on the dark web in May 2016. LinkedIn, in response, performs a 2 step authentication, which is the option of entering a pin code on your mobile device.

3. SECURITY IN VARIOUS STAGES OF SDLC

A. Phase Requirements

A software protection team member helps the majority of the team's members to make recommendationssecurity and specially advised as follows:-

1. Milestones of Cloud security
2. Criteria for exit

The advice is based on the size of the project, risks, and other factors. The member may be referred to as "Security Advisor." That member shall monitor the security elements in such a way that it does not face problems in later phases. This phase is the basis for how the security is implemented 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 design and architecture, ie the, guidelines are also included in the procedure. In addition to this, identification of the critical elements, the protection of which is of utmost importance is also included. 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 or may 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 with the idea that there should be a public source code, It is "Protection by obscurity" instead, but it does not do so information such as password of the users 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 must 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 Phase / Implementation Phase

A variety of steps have been taken to minimize and monitor security vulnerabilities in this process to ensure the release to end customers is as follows: Developers should be given careful attention in order not to create a high-priority menace with the wrong code. The implementation of testing and coding standards thus helps to avoid threats or faults to security. In addition, protection tools, such as "fuzzing," are used to detect errors by using standardized but non-valid inputs. Faults including buffer overflow, signed integer overflow, etc can also be detected with statical analytical tools. Includes both manual and automated code analysis for comprehensive reviews of code. The manual includes qualified developers to control the consistency of the code when automatically, including error detection software.

D. Deployment & Maintenance Phase

At this stage, the software is required to be secure enough to be ready for delivery to customers. The final security review is being conducted at this stage. In Final security review, the ability of the software and the vulnerability response is monitored, along with testing of penetration attack. It results in an overall picture of the security position of the software.

IV. SECURITY IN SDLC OVER CLOUD

The definition of software development for a project may vary, depending on various factors such as type, size and time. This paper analyses the method of cloud feasibility analysis and addresses security and risk concerns in the cloud-based cloud, making further use of the concept of combining SDLC with cloud in tandem with their cloud device. We plan to build a stable web application development.

This secure process can be described as a planned, built, checked, created, maintained, and provided with the best secure solution. Operation can not need to be linear; it can be sequential or iterative at the same time. In any web engineering operation module, we examine the safety requirement 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 controlling quality and mechanisms of maintenance. (Maintenance Module).

V. SECURE WEB APPLICATION DEVELOPMENT LIFE CYCLE(SWADLC)

We are looking at and resolving issues in security following discussion and research. We plan to update SDLC in Virtualized Environments for security implementation, such as cloud storage for different service growth scenarios. In terms of key points we suggested changes in SDLC in the mid-stages

In requirement analysis and feasibility study

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

In design and development
We process tasks via the Internet via a virtualized resource so that protected information exchange can be configured via a virtualized network and a secure link between the developer and the VM needs to be maintained.

In testing and configuration management

In this module we need to take care of individual and community testing.
1) Developer Side 2) Client Side

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

I. If we test it on the developer 's screen, then it must 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 need 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, we have to be cautious about security issues because many people are trying to disturb the design of module and codes by providing misfeedback at this stage.

A. Monitoring of Security 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)

Included in engineering activities are: We have identified operational activities common to all engineering activities of the modules:
Activities need to build a stable security approach Infrastructure practicality elicitation and description specifications.
Assurance Activities (AA): These activities include insurance actions like validation, verification as an issue validation, expert analysis for informed decision-making on the viability of designing and deploying services in various cloud infrastructures.
Management Activities(MA): These are further defined as: management activities

i. MA-OA (Organizational Activities)

Corporate activities are responsible for organisational policies, the creation of organisational roles and other web-based organisational activities in a virtualized environment. Project management tasks, project preparation and secure resource monitoring require assignment processes and use of different cloud infrastructures. The protection of security assurance, architecture and risk detection are assured by such virtualized tools, where activities are organised, controlled and monitored.

ii. Activities for Risk Identification(MA-RIA)

Identifying and managing safety risks is the biggest risk. Important operations are carried out in the safe production of software on the latest attack risk and rapidly rising cloud environments. It is the driver for successive operations such as security engineering, project management and security-related activities.

VI. CONCLUSION

We have now examined Secure Web Application Deployment Component for the Lifecycle creation of public and private clouds following safety and risk analysis in the SDLC cloud environment. Insert and insert the outcomes in the life cycle to facilitate decision-making as a "drive not transfer" as shifting decisions to save from one point to the next. This analysis will generalise the involving process which can be carried out during SDLC for improved cloud protection.

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.