https://doi.org/10.48009/2_iis_2006_73-76

APPLYING AGILE METHODOLOGIES TO IT SECURITY

Someswar Kesh, Central Missouri State University, kesh@cmsu1.cmsu.edu
Sandhya Jane, IT Consultant, jane.sandhya@ubs.com

ABSTRACT

Security threats to IT systems have become extremely dynamic, requiring a rapid response. Because of this, traditional life cycle approaches to IT security may not work. Agile methodologies provide a framework for rapid response in a dynamic environment. This paper discusses the fundamentals of agile methodologies and how they can be applied to IT security.

Keywords: Agile Methodologies, IT Security

INTRODUCTION

Information Technology is a vital component of today's enterprise, and it is virtually impossible to run a business without implementing comprehensive security solutions across an organization's entire IT infrastructure. Viruses, worms, security breaches and other malicious attacks on key business systems are getting more prevalent and sophisticated. New legislations like Sarbanes-Oxley and Health Insurance Portability and Accountability Act (HIPPA) require organizations to maintain a high level of IT security. Therefore, security is no longer an afterthought: organizations need to respond to security threats quickly and comprehensively. This indicates that organizations need to look at new methods for managing IT security [2].

Until a few years ago, organizations had the luxury of taking weeks, or even months, to apply a security patch to a system. Today, new security threats are appearing more quickly and attacks spreading more rapidly, having significant global impact within hours, if not minutes. Dynamic security threats cannot be faced with a static security process. Today's business needs demand a security process that can squelch most attacks before they can cause damage and the agility to apply effective countermeasure. Agile methods are a response to this expectation. While agile methodologies have been mostly used for software development, the concepts and processes of agile development can be very useful to security. This research demonstrates how agile methodologies can be used to combat security threats in organizations.

FUNDAMENTAL CHARACTERISTICS

The goals of agile methodologies are to increase the speed of response and reduce the cost of software development. To achieve this, the first delivery should be made in weeks and should be followed by a rapid feedback. Design quality is improved continually, followed by constant testing. This reduces the need for more expensive error detection at very late stages. Since agile methods have shown to improve quality, due to short iterations and quick releases, their adoption is likely to significantly improve IT security [3].

The most important characteristics of agile methodologies are as follows:

- **Individuals and interactions over processes and tools:** While other methodologies may get bogged down with processes, the individuals involved are of far greater importance in agile methodologies than tools. Furthermore frequent interactions between individuals reduce the chances of errors and misunderstanding due to lack of communication.

- **Working systems over comprehensive documentation:** While documentation is still done, avoiding comprehensive documentation assists in reducing the need for paperwork. The focus then should be on developing working systems rather than documentation.

- **Users and designers collaboration over contract negotiations:** When both users and designers collaborate over contract negotiations, it results in better systems development.

- **Responding to change over following a plan:** Flexibility is the key to agile systems development. While some planning process is required, it is not as rigid as the structured development methodologies.

IMPORTANT STEPS FOR AGILE IT SECURITY PROJECT MANAGEMENT

In order to cater to the above characteristics, agile methodologies need to follow certain steps. These steps are discussed next.

- Face-to-face conversation is the preferred method of communication. Relevant documentation needs to be written down. The document should be primarily important information only.

- The best architectures, requirements and designs emerge from self-organizing teams. Project teams must have people mature enough and the right skill level to develop the best security designs and architectures. The broad architecture especially needs to be developed at an organization or company level. If this were left to individual teams, the result would be overlapping technologies and chaos at the company level.

- At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly. Teams should constantly strive to understand their strengths and weaknesses and how the project management processes can be improved. The process also believes these recommended changes should also be surfaced to the organization so that the improvement ideas can be leveraged by the entire staff. [1]

- In agile methodologies, it is recommended that large projects be decomposed into smaller ones. Each small project can delivered quickly and repetitively. Both users as well as developers will have to interface with each other and work as a team to make the project successful.

- The primary measure of progress is a working documentation. This should be done at the end of each iteration cycle.

- Agile processes promote sustainable development. The sponsors, team members and users should be able to maintain a constant pace.

- Technical excellence and good design are essential. However, if design work is shortchanged because of cranking out quick fix solutions, this can be problematic.

- System designers and management should focus on delivering the core requirements first. This "maximizes the work not done." It also allows critical security systems to be delivered more quickly.

- The best architectures, requirements and designs emerge from self-organizing teams. Project teams must have people mature enough and the right skill level to develop the best security designs and architectures. The broad architecture especially needs to be developed at an organization or company level. If this were left to individual teams, the result would be overlapping technologies and chaos at the company level.

HOW TO IMPLEMENT AN AGILE SECURITY METHODOLOGY

Security Team Formation

As discussed before, two critical requirements for the initiation of an agile methodology is to assign security teams and decompose the project into smaller deliverable components. Formation of teams requires the identification of stakeholders for security. Typically, in an organization everyone is a stakeholder. Stakeholders can be classified into whether they are internal or external to an organization. Both internal users as well as external users should be made part of the team. Examples of external stakeholders are vendors of an organization. Internally, team members should also be composed of people who deal directly with security and those who do not. Both groups should be adequately represented. The Chief Information Officer (CIO), Chief Information Security Officer (CISO), network and systems administrators, database administrators, and programmers are those that directly interface with I.T. Identifying and classifying users internal to an organization but those that are not directly responsible for administering the I.T system can be greatly assisted by the use of Porter's value chain model [4], which provides a classification scheme of users by grouping them based on the activities they perform. Guidelines for the initial team formation should be accomplished at the highest levels of the organization to avoid unnecessary duplication, but be comprehensive and represent various groups of stakeholders. If the security team was formed as a response to a negative security incident in the organization, then it should assure the organization that something is being done.

It takes a wide range of professionals to support a diverse information security program. Because a good security plan should be implemented across the entire organization, small and agile teams are the key component and vital force driving the successful implementation of an information security program. To develop and execute specific security policies and procedures, additional teams may be required. Finally, technical expertise is necessary to implement the details of the security operation.

Project Decomposition

The teams formed should decompose the security project into smaller, manageable projects. These may be referred to as phases. The phases for IT security can be referred to as initiation, analysis, development/acquisition, and operations/maintenance. These phases are discussed next. The teams should ensure that they meet frequently to ensure proper progress and information dissemination.

The initiation phase begins with a directive from upper management specifying the process, outcomes, and goals of the project, as well as its budget and other constraints. Frequently, this phase begins with the affirmation or creation of security policies on which the security program of the organization is or will be founded. This also becomes the Information Security Blue Print. Teams of managers, employees, and consultants are assembled to analyze problems, define their scope, specify goals and objectives, and identify any additional constraint not covered in the enterprise security policy. Finally, an organizational feasibility analysis determines whether the organization has the resources and commitments to conduct a successful security analysis and design [5].

In reality, many information security projects are initiated in response to a significant negative event within an organization. While these circumstances may not be the ideal conditions under which to begin work on an organization's information security posture, the agile process is the best way forward; the security team should emphasis that improvement is now underway.

In the analysis phase the documents from the investigation phase are studied. The team created during the investigation phase conducts a preliminary analysis of existing security policies or programs, along with documented current threats and associated controls.

This phase also includes an analysis of relevant legal issues that could affect the design of the security solution. Increasingly, privacy laws are a major consideration when making decisions about information systems that manage personal information. Recently many state legislatures have made illegal certain computer-related activities that were once unregulated, so a detailed understanding of these issue is vital.

The risk management task begins in this stage. Risk management is the process of identifying, assessing, and evaluating the levels of risk facing the organization: specifically, the threats to the organization's security and to the information stored and processed by the organization [6].

Once the initiation and analysis phase is completed, then the design, development and implementation starts. The entire project is broken down to smaller projects with small teams assigned to each project. These agile teams then work on their respective projects to quickly roll out a working system.

Each team then designs, programs, develops or purchases systems with the basic requirements/features for their respective projects as quickly as possible. The teams then review the systems, take user feedback and business needs to refine the system, and add features to further improve the solution.

CONCLUSIONS

Behind the agile approach is the belief that change is the only constant. Agility is dynamic, context-specific, and growth-oriented—embracing changes aggressively. It is about succeeding and winning in an ever-changing security environment.

Today, information security systems need constant monitoring, testing, modifying, updating, and repairing. Traditional applications systems are not designed to anticipate a vicious attack that requires some degree of application reconstruction as a normal course of operation. In security, the battle for stable, reliable systems is a defensive one. As new threats emerge and old threats evolve, the information security profile of an organization requires constant adaptation to prevent threats from successfully penetrating sensitive data. This is where agile methodology is most suited for organizations IT security needs.

Agility, ultimately, is about creating and responding to change. What is new about agile methods is not

only the practices used, but the recognition of people as the primary drivers of project success, coupled with an intense focus on effectiveness and maneuverability.

Agile IT security addresses two pressures that characterize today's business and technology world: the need for dynamic, innovative approaches to security threats, which in turn allows an organization to run their daily business and concentrate on their core competencies and overall business benefit.

REFERENCES

1. Beck, K. et. al (2005). *The Manifesto for Agile Software Development*. http://agilemanifesto.org
2. Denzel, N. (2005). *Safeguard Your Business with HP Security Solutions*.http://h50043.www5.hp.com/hpservices/ap_features/july04/75600.htm
3. Highsmith J. & Cockburn, A. (Nov 2001). Agile software development: The business of innovation, *IEEE Computer*, 131-133.
4. Laudon, K.C.& Laudon, J. (2004). *Management Information System- Managing the Digital Firm*, Upper Saddle River, NJ: Pearson Prentice Hall.
5. Swanson, M. & Guttman, B. (1996), Generally accepted principles and practices for securing information technology systems, *National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce NIST Special Publication 800-14*.
6. Whiteman, M. & Mattord, H. (2004). *Management of Information Security*, Boston, MA: Thomson Course Technology.