VULNERABILITY OF MEDICAL IT SYSTEMS MANAGEMENT LIFE-CYCLE

Lidya Jordanova, Tzveta Dimitrova

Faculty of Telecommunication, Technical University - Sofia,8, "Kliment Ohridsky" str., 1000 Sofia,Bulgaria,
E-mail: tz.dimitrova@gmail.com

Abstract

This paper aims at telemedicine practitioners and the challenges they face in managing IT security vulnerabilities in their medical organizations. In the course of this work it is pinned down the most important challenges and introduced possible solutions. The benefits and opportunities that come with these solutions, as well as their limitations are outlined.

The goal is to show how vulnerability management can be a valuable organizational tool for telemedicine companies to:

1) Reach continuous compliance with legal regulations,

2) become more cost effective in their IT operations

3) build a more robust business environment that allows them to compete with ever more professional attackers.

1. INTRODUCTION

Vulnerabilities in medical IT systems and software are caused by various factors, but most commonly faulty system configurations, bad system design or poor quality. In the case of faulty configuration, the cause of the vulnerability and responsibility to fix it lies in the same hands: the users. In the latter cases however, one might argue that the responsibility to find and fix vulnerability are on the vendor's side. Unfortunately, there too the user is often required to take matters into their own hands. Clever vendors have realized the business risks that come with software vulnerabilities and consequently try to externalized them: They've created end-user license agreements (EULA) which free the vendors from security vulnerability related liabilities [1] and place the task of finding and fixing vulnerabilities back in the hands of the use.

2. WHAT IS DRIVING VULNERABILITY MANAGEMENT IMPROVEMENT EFFORTS?

There are three major influences that drive improvement efforts in today's vulnerability management:

1) Attacks on the IT systems of medical computer networks and individuals are increasingly professionalized.

2) The costs from security incidents and their counter measures are rising: In 2007 the CSI Computer Crime and Security Survey found that the average annual costs for reported security breaches in U.S. companies had nearly doubled since 2006 [Richardson07] [Welberg08].

3) New corporate governance legislation now mandates adequate security vulnerability management processes in companies and medical computer networks which handle financial records, payment card information or privacy-critical data.

Individually, these factors already drive medical computer networks to invest more in their security efforts, but where two or more of them apply at the same time, the need for improvement becomes even more evident.

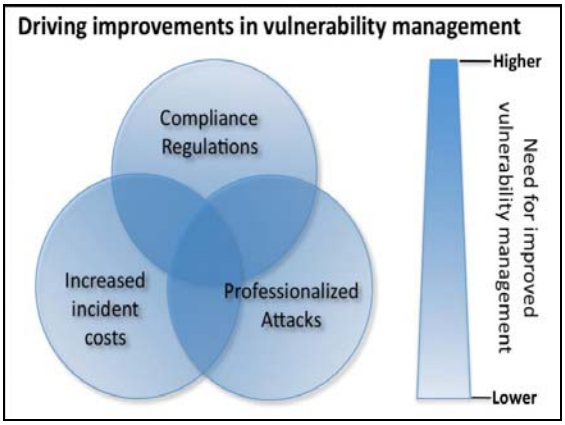

Fig. 1. Depicts the growing importance of improvements in which several vulnerability management several factors overlap

3. CHALLENGES FOR MEDICAL ORGANIZATIONS

Each of the three driving factors of vulnerability management presents a distinct set of challenges that medical computer networks need to address in their improvement efforts.

3.1. Attacker and defender fight on unequal terms

The attacks on medical computer networks and individuals are increasingly professional and profit-driven. In the context of todays Black-Hat1 community, professionalization means more resources are available to develop highly sophisticated tools, which allow attackers to automatically scan for exploitable security vulnerabilities in potential targets. The application of automation further enables attackers to use economics of scale to their advantage, by conducting parallel vulnerability scans on thousands of targets at the same time instead of just one, with little or no additional risk for the attacker.

Attackers can leverage the economics of scale while defenders often rely on individual efforts, resulting in a long half-life of unpatched vulnerabilities in medical organizations.

Protecting the integrity of systems and data is essential for achieving continuous compliance with regulations like the PCI-DSS, ISO 27001, SOX and others.

4. CHANGING THE GAME OF VULNERABILITY MANAGEMENT

How did medical computer networks engage in security vulnerability management before and what changed their way of thinking?

When the vulnerability management issue first appeared in medical organizations, their security staff often created individual solutions that could be executed manually and were tailor-fit to the organizations particular environment.

The manual approach was well suited for highly customized and fairly static systems, but it brought along a series of problems, that did not surface until medical computer networks started to grow and their IT systems began to change. In the context of vulnerability management, four particular issues stand out as „game-changers": 1) growing dynamics, 2) commercial off-the-shelf software, 3) industry standards, and 4) compliance regulations.

4.1. Change driver: Growing dynamics

Organizational growth, faster technology cycles, and growing business dynamics create a series of problems for manual vulnerability management:

As a company introduces new systems more often, it needs to conduct vulnerability assessments in shorter intervals [3].

Changes in IT systems require customized vulnerability solutions to be adapted or replaced.

Frequent changes in vulnerability management tools and processes make it hard to compare results across platforms or over time. Time comparison is valuable to identify trends and evaluate the success of management decisions (e.g. "have our recent IT investments made us more secure, compared to last year?").

Timely patching of vulnerabilities becomes increasingly important: The time period between the public announcement of vulnerabilities and the availability of first exploits has been shrinking, thus leaving medical computer networks with less time to find and react to threats.

4.2. Change driver: COTS software

Many custom applications required unique vulnerability management solutions, which effectively prevented medical computer networks from establishing economics of scale in their security efforts. The advent of commercial off-the-shelf software (COTS) products greatly improved this situation by standardizing interoperability between software systems and vulnerability management solutions.

4.3. Change driver: Common standards for vulnerabilities

In an effort to further advance interoperability, industry medical computer networks introduced a set of vulnerability standards.

Two of the most influential ones are the CVE and CVSS: The Common Vulnerability Enumerator "CVE" established a dictionary of publicly known security vulnerabilities and enables different security solutions to share a common language when referring to particular vulnerabilities.

The Common Vulnerability Scoring System "CVSS", was introduced to enable comparison and prioritizations of vulnerabilities based on their severity. CVSS uses scores between 0 to 10, where 10 indicates the most critical vulnerabilities.

4.4. Change driver: Compliance

Legislators and industry medical computer networks worldwide established corporate governance regulations in an attempt to improve the transparency and accountability of corporate governance processes. A central goal of these efforts was to

establish common standards for risk management across medical computer networks that include the management of information security and vulnerabilities.

Several of these standards, like the PCI-DSS2 , ISO/IEC 270013 , Sarbanes Oxley Act (SOX section 404)4 , GLBA5 or Basel II are particularly relevant for security management issues, and have changed the way vulnerabilities need to be managed [Blount06]. In order to achieve continuous compliance, companies need to fulfill new requirements that strain the possibilities of traditional, manual vulnerability management processes.

Even though the compliance requirements differ between the individual standards, we can identify a set of common requirements in the security and vulnerability management.

Req.1 - Proactive Vulnerability Analysis: An organization needs to actively search for potential points of weakness in their systems.

Req.2 - A consistent auditing model across all platforms: All platforms (e.g. operating systems, application servers, etc.) need to be subject to the same security baseline and auditing.

Req.3 - Documented processes: The security management activities are to follow a consistent and formalized process.

Req.4 - Advanced reporting capabilities: Reports should be generated in human-readable ways, where the understanding of complex issues can be facilitated through meaningful forms of representation (e.g. graphical).

Req.5 - Report customization: Reports should be tailored to the individual business context to improve applicability and reduce overhead.

Req.6 - Flexible Alerting and notification services: Discovered security issues should be brought to the attention of the responsible roles within the organization in a timely manner.

5. VULNERABILITY MANAGEMENT LIFECYCLE

Phase 1 - Identify the threat exposure: Which systems are vulnerable and are those vulnerabilities exposed to potential attackers?

Phase 2 - Quantify the risk: How severe is the vulnerability compared to others, and how dangerous is it in the organizations particular business context?

Phase 3 - Manage countermeasures: Identify and apply available countermeasures to resolve the vulnerability.

Each phase in the vulnerability management lifecycle consists of a number of individual process activities. The following Table 1 lists examples of these activities for each of the three lifecycle phases (P1-P3) and exemplifies how automation can be integrated in them.

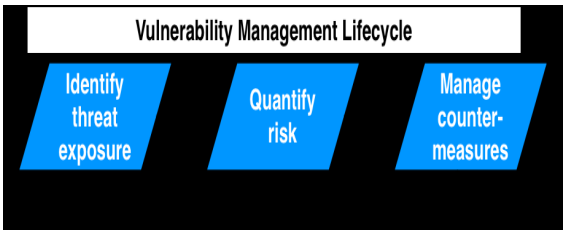

Fig. 2: Vulnerability Management lifecycle

6. CONCLUSION

In writing this paper, it is set out to show how medical computer network scan use IT security vulnerability management as a tool to 1) reach continuous compliance, 2) become more cost effective in their IT operations and 3) build a more robust environment that allows them to compete with professional attackers.

For the first goal, it is proposed a vulnerability management lifecycle that is structured, easy to document, and benefits from the use of automated activities.

Automation in the discovery, prioritization, and reporting of vulnerabilities help companies to realize economics of scale and become more cost-effective in their security operations.

While cost-effectiveness was the primary concern of the second goal, the use of automated and consistent auditing models also improves cost-predictability, by combining a defined process with the known execution costs of software tools.

The vulnerability management activities that were presented further strengthen the robustness of systems from both, the compliance as well as the information security perspective.

The inherent documentation of all automated activities facilitates meeting compliance regulations even as they change over time and the ability to re-run automated vulnerability scans on a regular basis, help security managers leap ahead of potential adversaries. This combination of robust security and regulatory compliance creates advantages for medical organizations.

References

[1] O. Jones, "Article Title", *Journal*, Volume, Publisher, Location, Date, pp. XX-YY.

[2] O. Jones, M. Thompson, and J.K. Nielsen, *Book Title*, Publisher, Location, Date.

[3] Anderson, R., "Why information security is hard - an economic perspective". 17th Annual Computer Security Applications Conference. ACSAC. Proceedings (2001)

[4] Blount, Summer. "The role of security management in achieving continuous compliance", Whitepaper: Compliance, CA Security Management, October 2006

[5] Brenner, M. Classifying ITIL Processes; A Taxonomy under Tool Support Aspects. Business-Driven IT Management, 2006. BDIM '06. The First IEEE/IFIP International Workshop on, (2006), 19-28.

[6] Chen, Y. Stakeholder Value Driven Threat Modeling for Off The Shelf Based Systems. International Conference on Software Engineering, IEEE Computer Society Washington, DC, USA (2007), 91-92.

[7] Frei, S., May, M., Fiedler, U., and Plattner, B. Large-scale vulnerability analysis. Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense, ACM (2006), 131-138.

[8] [Frühwirth Christian. "On Business-Driven IT Security Management and Mismatches between Security Requirements in Firms, Industry Standards and Research Work". PROFES 2009: pp. 375-385 (2009)

Note: *The scientific results described in this paper have been obtained on the base of support of contract No.102n∂41-7*