УДК 004.771
ГРНТИ 20.53.01

АУДИТ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ И ИСПОЛЬЗУЕМЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

Сенькив Д.А.
магистр, аспирант-соискатель
Нижегородский государственный технический университет им. Р.Е. Алексеева
(ул. Минина, 24, Нижний Новгород, Нижегородская обл., 603950)

AUDIT AS A MEANS OF ENSURING INFORMATION SECURITY OF WEB APPLICATIONS AND USED COMPUTER SYSTEMS

Senkiv D. A.
Master degree
Nizhny Novgorod State Technical University n.a. R.E. Alekseev
(Minin St., 24, Nizhny Novgorod, 603950)

Аннотация. При обеспечении информационной безопасности (ИБ) веб-приложений с использованием компьютерных систем особое значение имеют процессы контроля и средства защиты, а также выявление уязвимостей в существующей системе. Аудит ИБ позволяет осуществить контроль процессов и выявление уязвимостей. В большинстве работ очень мало внимания уделяется системной классификации мероприятий аудита и тестированию как одному из основных типов аудита ИБ. Мероприятия, связанные с тестированием существующих систем, рассматриваются в однобоком виде лишь в качестве тестирования на проникновение или инструментального аудита. Проведение такого типа аудита не регламентируется каким-либо системным подходом. Целью работы является систематизация основных сведений об этапах, теоретических и практических подходах к аудиту ИБ, классификации мероприятий аудита.

Abstract. When ensuring information security (IS) of web applications using computer systems, control processes and protection tools, as well as identifying vulnerabilities in the existing system, are of particular importance. IS audit allows you to control processes and identify vulnerabilities. In most works, very little attention is paid to the systemic classification of audit activities and testing as one of the main types of information security audit. Activities related to testing existing systems are considered one-sided only as penetration testing or instrumental audits. This type of audit is not regulated by any systematic approach. The aim of the work is to systematize the basic information about the stages, theoretical and practical approaches to IS audit, classification of audit activities.

Ключевые слова: информационная безопасность, аудит, тестирование на проникновение, аудит информационной безопасности, тестирование, информационно-технические меры, защита информации, превентивный анализ

Keywords: information security, audit, penetration testing, information security audit, testing, information technology measures, information protection, preventive analysis

Introduction

New information technologies are being introduced into all spheres of life and ensuring IS is an indispensable part of this process. The use of computer technology and telecommunication systems, as well as an increase in the amount of processed information, contribute to the expansion of the possibilities of unauthorized access to resources and data of computer systems.

IS is the process of ensuring the availability, integrity and confidentiality of information.

The process of ensuring IS is constantly becoming more complex. This is due to the increasing complexity of computer systems and their security systems, heterogeneous networks and an increase in the number of thin clients, wearable electronics - smartphones, smart watches, tablets.

Hacks into computer systems are becoming more sophisticated and often have irreversible consequences for companies and organizations.

Usually people think about ensuring IS of resources in three cases:

- when developing / designing the system;
- after development / design of the system;
- after an incident of IS, which caused the user or the company losses - financial, reputation, temporary.

First of all, the goal is to ensure IS, for example, to give guarantees to users and ensure the protection of their systems and data, obtaining a certificate of conformity (for example, PSI DSS - Payment Card Industry Data Security Standard), compliance with the IS standard ISO / IEC 27001.

Based on the goals and tasks performed in the computer system, various measures and degrees of protection will be developed.

For example, if a computer system is used only as a means of surfing the Internet, then of the necessary means for ensuring security, first of all, will be the use

of anti-virus protection, as well as compliance with basic safety rules when working on the Internet [1].

In another case, if a selling site or a game server is located on a computer system, then the necessary protection measures will be completely different.

Knowledge of the potential threats, as well as the security vulnerabilities that these threats typically exploit, is essential in order to select the most appropriate security controls.

Before you start organizing IS, you need to answer three questions:

1. What needs to be protected? User workstations or remote server?
2. From whom to protect, which threats will be predominant - external or internal? Which scenario is more dangerous - employee data theft or system hacking?
3. How to protect, by what methods and means? Use proprietary software or free software? Protect your system in real time or conduct regular scans and audits?

After answering these questions, you can draw up a more clear strategy for protecting a certain type of system, select the most optimal and effective protection methods.

Then it is necessary to audit the current solution, system.

Information security audit

IS audit - an independent assessment of the current state of the IS system, establishing the level of its compliance with certain criteria, and providing the results in the form of recommendations.

IS audit allows you to get the most complete and objective assessment of the security of a computer system [2], localize existing problems and develop an effective program for building an organization's IS system. As part of an IS audit or as a separate project, penetration testing can be carried out to test the ability of a company's information system to resist attempts to penetrate the network and improperly influence information.

Audit goals can be divided into:

- preventive - aimed at proactive identification of threats and vulnerabilities and prevention of IS incidents;
- detecting - aimed at detecting new or clarifying the features of existing threats and security vulnerabilities during or after IS incidents;
- corrective - aimed at the formation of a set of measures to improve the effectiveness of the existing protection system after IS incidents, taking into account newly identified threats and vulnerabilities.

The audit is divided into several conventional categories:

1. Web application security audit

The site is tested for vulnerabilities by testing for resistance to combined attack methods [3] and is based on OWASP (Open Web Application Security), WASC (The Web Application Security Consortium), OSSTMM (Open Source Security Testing Methodology Manual), PTES (Penetration Testing Execution Standard) methodologies) and PCI DSS best practices and recommendations. All work is supported by extensive practical experience of specialists.

In most cases, vulnerabilities from the OWASP TOP 10 list are identified; in 80% of cases, the detected vulnerabilities are critical, allowing unauthorized access to confidential information or to the server.

An audit of a resource (web components and web environment), as a rule, is performed using the «BlackBox» method and includes the following stages:

- passive collection of information;
- definition of the web environment;
- platform definition;
- CMS type definition;
- port scanning;
- collection / search for public exploits;
- automatic scanning;
- data analysis;
- identification of resource bottlenecks;
- collection and analysis of the information received;
- analysis of attack vectors;
- confirmation of the received vectors;
- compilation of a report.

Site audit in «BlackBox» mode simulates a real hacker attack on the customer's site without destructive consequences.

During the site audit, the following actions are performed on the tested resource:

- search for vulnerabilities of server components;
- search for vulnerabilities in the server web environment;
- check for remote execution of arbitrary code;
- checking for overflows;
- checking for injections (code injection);
- attempts to bypass the web resource authentication system;
- checking a web resource for XSS / CSRF vulnerabilities;
- attempts to intercept privileged accounts (or sessions of such accounts);
- attempts to make Remote File Inclusion / Local File Inclusion;
- search for components with known vulnerabilities;
- check for redirection to other sites and open redirects;
- scanning directories and files using brute force;
- analysis of search forms, registration forms, authorization forms, etc .;
- race condition attacks;
- guessing passwords.

At the end of the audit, a detailed report is provided with the identified vulnerabilities, recommendations for elimination, examples of attacks and descriptions of possible penetration scenarios.

2. Penetration testing of the network perimeter

Penetration testing is a popular worldwide way to assess the security status of a network perimeter. The essence of such tests is an authorized attempt to bypass the existing complex of information system protection means. During testing, a security analyst plays the role of an attacker motivated to violate the IS of the customer's network. The provision of penetration

testing services is based on OSSTMM, PTES methodologies and includes:

- passive collection of information;
- port scanning;
- determination of types and types of network equipment;
- definition of types and types of operating systems in the network infrastructure;
- definition of types and types of adjacent peripherals in the network infrastructure;
- definition of types and types of specialized devices or their combination;
- collecting banners and searching for public exploits;
- collection and analysis of the information received;
- definition of «entry points»;
- description of attack vectors;
- attempts to exploit;
- confirmation of the received vectors;
- compilation of a report.

3. Stress Testing

Stress testing («load-testing») - is necessary to determine or collect performance indicators and response time of a software and hardware system or device in response to an external request in order to establish compliance with the requirements for this system (device) [4].

To investigate the response time of the system at high or peak loads, «stress testing» is performed, in which the load placed on the system exceeds the normal scenarios of its use. A modern IT infrastructure must provide the required level of performance. Any disruptions, delays and rejections can lead to the loss of customers, both current and potential. The main purpose of load testing is to monitor the system performance by creating a certain expected load on the system (for example, through virtual users).

When conducting stress testing, it is necessary to define test scenarios containing the values of the design and expected peak performance of the system. Each scenario is based on the following data:

- object of testing;
- testing objectives;
- the purpose of testing;
- requirements;
- specifications;
- regulations.

Any software or server software must run under load for a long time. System failures and failures can lead to losses, loss of customers and other unpleasant consequences [5]. Load testing allows you to determine how and at what speed an application is performing under a certain load. Through load testing, the compliance of the product's performance with the requirements formulated in the specification and design documentation is assessed.

4. Compliance with PSI DSS standard

To obtain a PCI DSS certificate of compliance, companies working with international payment systems Visa and Mastercard must comply with the requirements of the standard. Such requirements include the following procedures:

- monthly check of security components;
- monthly check of system components of servers;
- monthly external ASV scan;
- quarterly analysis of wireless networks;
- quarterly internal scanning;
- annual internal and external penetration test;
- annual identification of new threats and revision of IS policies;
- annual briefing of IS department employees;
- annual analysis of publicly available web applications;
- every six months revision of the rules for firewalls and routers;
- annual review and monitoring of the performance of video surveillance systems;
- annual testing of the IS incident response plan.

After the audit, it is necessary to comply with as many of the received recommendations as possible and initiate a re-audit [6]. When the required level of security is achieved, conduct an audit in the future with a certain frequency (for example, once a month).

Conclusion

The concept of IS, its components and procedures necessary to determine the current level of security, ways to increase it were considered.

Audit is one of the basic actions aimed at ensuring IS. An independent assessment of the current state of the IS system establishes the level of its compliance with certain criteria, and provides the results in the form of recommendations.

An audit allows you to reduce the risk of confidential information leakage, increase control over IT and IS departments, as well as build the necessary level of protection for sensitive company information.

An audit is a basic procedure for ensuring the level of IS of a computer system and allows you to identify and eliminate obvious and gross errors made in the design and configuration of a computer system. The use of audit is advisable in a computer system of any scale. Together with other basic procedures, audit can prevent most cases of penetration into the system.

List of references

1. Бондарев В. В. Введение в информационную безопасность автоматизированных систем: учебное пособие – М.: МГТУ им. Н. Э. Баумана, 2018. [Bondarev V. V. Introduction to information security of automated systems: schoolbook - M.: BMSTU n. a. N.E.Bauman, 2018; (In Russ).]

2. Бирюков А. А. Информационная безопасность. Защита и нападение/А. А. Бирюков - М.:ДМК Пресс, 2017. [Biryukov A. A. Information security. Defense and attack - M .: DMK Press, 2017 (In Russ).]

3. Кочешков А. А., Сенькив Д. А. Информационная безопасность публичных облачных сервисов /А. А. Кочешков, Д. А. Сенькив // Научно-Технический Вестник Поволжья, Казань. – 2020. – № 7 – с. 70 – 72 [Kocheshkov A. A., Sen'kiv D. A. Informacionnaja bezopasnost' publichnyh

oblachnyh servisov - Nauchno-Tehnicheskij Vestnik Povolzh'ja, Kazan, 2020;7:70-72. (In Russ).]

4. Boyce G. Linux Networking Cookbook/G. Boyce - Packt Publishing. – 2016.

5. Астахов А. Введение в аудит информационной безопасности/ GlobalTrust Solutions. URL: http://globaltrust.ru [Astakhov A. Vvedenie v audit informatsionnoi bezopasnosti/GlobalTrust Solutions. URL: http://globaltrust.ru]

6. Скабцов. Н. Аудит безопасности информационных систем — СПб.: Питер, 2018.[Skabtsov. N. Audit bezopasnosti informatsionnykh sistem — SPb.: Piter, 2018 (In Russ).]