Computer Security: Risk Management Methodologies in Information Technology Systems

Debora C. Faria[1]

Abstract

This article aims to demonstrate risk management methodologies in a practical and applicable way, and how its processes are useful for an organization to be able to estimate and evaluate treats and risks that may affect its business. Managing the security infrastructure, as well as the business value they generate, has proven to be the main challenge of IT departments in the last years. However, today's infrastructures have high levels of integration and are open to increasingly hostile environments that require fast and accurate responses to incidents that can import risk of harm to businesses. Most of the time, organizations are not prepared enough to react effectively to threats, in other words, in a short time manner to prevent their business from being harmed. Characterized by the preservation of confidentiality, integrity and availability of information, the security of information protects the main assets of an organization aiming at continuity, minimization of damages and maximization of business opportunities and investments. The main source of an organization has for identifying its security requirements is derived from risk assessment, which is part of the overall and ongoing risk management process, whose purpose is to reduce risks to compliance levels to the organization.

Keywords: Information Security, Vulnerabilities, Risk Management.

Introduction

Information Security protects information against threats to ensure continuity, minimize damage and maximize business investments and opportunities. It can be achieved by using policy controls, practices, procedures, organizational structures, and hardware and software infrastructures. It is characterized by the preservation of confidentiality, integrity and availability of information, and aims to preserve the competitiveness, billing, profitability, compliance with legal requirements and the image of the organization.

There are three main sources for an organization to identify its security requirements. The first is the set of principles, objectives and needs for the processing of information that an organization developed to support its operations. The second is the current legislation, image, regulations, and contractual clauses that the organization, its partners, contractors, and service providers must attend. The previous two are used as references to develop the main source of security requirements, which is derived from risk assessment, process responsible for identifying threats to assets, vulnerabilities with their respective probabilities of occurrence and business impacts.

[1] Debora C. Faria, student of the Analysis and Systems Development course at Fatec SJC - Faculdade de Tecnologia de São José dos Campos.

Evolution of Cyber Attacks

Identifying the cyber-attacks that had the most impact in the last three decades, which show the evolution of cyber-attacks and the constancy of techniques such as social engineering and malware distribution through pirated software. Below are some examples:

I. CIH/Chernobyl (1998): Originally from Taiwan, this is considered one of the most harmful viruses in history because of the millions of dollars of losses that has caused worldwide, and the speed with which it has spread. His modus operandi was lethal: once installed on a computer, it deleted all information from the entire computer, even corrupting the bios so that the system could not boot. It is estimated that it has affected more than 60 million Windows 95, 98, and ME users.

II. Stuxnet (2010): is the first known example of a cyber warfare weapon, as it was designed to attack Iran's critical infrastructure. This worm, which spread through removable USB devices, carried out a targeted attack against companies with SCADA systems, with the aim of collecting information and then ordering the system to self-destruct. It exploited the vulnerability of Windows MS10-046, which affected shortcuts, to install itself on the computer, specifically in Windows 2003, XP, 2000, NT, ME, 98, and 95. It was also able to log into devices that were not connected to the Internet or to a local network.

III. Mirai (2016): Is the widest known botnet behind major denial of service (DDoS) attacks up to date. This botnet affected major companies such as Twitter, Netflix, Spotify and PayPal. This malware has infected thousands of IoT devices, remaining inactive within them. Mirai creators activated it on October 21, 2016, using it to attack DNS service provider Dyn. Both their services and their customers have fallen or faced problems for hours.
It was created for the initial purpose of taking down Minecraft servers.

IV. Ryuk (2019): Ryuk ransomware jeopardized the critical infrastructure of large national and international companies in the last quarter of 2019. Among his victims are the city hall of Jackson County, Georgia (USA). This malware, whose origins are associated with the Russian group Grim Spider, encrypts the files on infected devices, and only allows the victim to recover his files if he pays a ransom in bitcoins. Ryuk appears to be derived from Hermes, a similar piece of malware that can be purchased on the dark web and customized to meet the needs of the buyer.

Information Security Monitoring

A substantial number of suspicious events occur within most corporate networks every day and go completely unnoticed. Only with an effective security monitoring strategy, an incident response plan, validation and metrics in the right place, with properly configured tools, that a good level of security will be achieved.

The idea is simple, to have an automatic relationship to present events and vulnerabilities, to build intelligence in security tools so that we have alerts of events that have occurred, occurring, or symptoms of future attacks.

For this to occur, you must:

- Define escope of monitoring security and logs in general by means of a management strategy;
- Integrated incident response plan;
- Validation exercises and attacks against security controls;
- And control of safety metrics aiming at the measurement and evaluation of improvements.

Security monitoring involves real-time monitoring of events and activities always happening across all important systems in your organization. To properly monitor an organization, through technical events that can help to an incident or an investigation, a product such as SIEM - Security and Event Information Management is typically used.

These tools are used by security analysts and managers to filter tons of data and identify and focus only on the most relevant events.

In addition, it is necessary to understand regulatory impacts of each event and alerts on your company, as well as a planning and deep understanding of the amount of data that the system will be required to handle. These points are important for monitoring not only invasion compliance, but laws and rules.

The best records can be stored, investigated and correlated, improving the possibility of detecting an incident and mitigation time. The need to respond to incidents, identify anomalous or unauthorized behavior, and protect intellectual property today has never been more critical. Without a solid log, a correct management strategy and treatment, it becomes almost impossible to have the data needed to conduct a forensic investigation, and without tools to monitor, identify threats and respond to attacks against confidentiality, integrity or availability, become much more difficult.

Some important points for an incident response or forensic investigation to be successful iskey:

- Acquire and store asset logs from networks, software, and other devices and assets as much as possible, providing research and restore their capabilities for analysis;
- Monitor events of these assets in real time as much as possible;
- Perform regular vulnerability scans on your hosts and devices and correlate these vulnerabilities to intrusion detection alerts or other critical events, thereby identifying high-priority attacks, and how they happen by minimizing false positives;
- Aggregate events by normalizing data from independent network devices, and tailor the security of devices and application servers into usable information;
- Analyze correlated information from various sources, such as vulnerability scanners, IDS, IPS, firewalls, servers, and so on. In order to identify attacks as soon as possible;
- Review and periodic forensic analysis in historical events or in real time through visualization and repetition of events;

- Creation of customized reports to better visualize your organizational security;
- Make performance and performance adjustments on safety devices periodically to provide increased speed inanalysis.

Infosec Teams

The idea behind infosec teams is to understand security as a constant concern, from development to software implementation andmaintenance.

Each team is represented by a color of the chromatic circle. They are:

Red Team - The red team consists of "authorized hackers". His role is to find vulnerabilities in the application that can be exploited for malicious purposes. To do this, this team uses attack techniques with authorization from the organization and maps the vulnerabilities found to be fixed.

Blue Team - While the red team must attack the application to expose vulnerabilities, the blue team has the role of defending and anticipating these attacks. He is responsible for the security of the entire infrastructure of the organization and has as functions the mapping of risks, damage control, incident response and operational security.

Yellow Team - This is the team of developers. Their tasks involve backend performance, application functionality, and user experience.

Purple Team - The purple team consists of the interactions between the red and blue teams and aims to maximize the results of the red team and improve the responsiveness of the blue team. Thus, the purple team integrates the results of the security tests with the defense capability of the organization.

Orange Team - Interactions between the red and yellow teams are part of orange team. These interactions are important for educating developers to program safely. Because the activities of the red team involve attacking the application built by the yellow team and exposing vulnerabilities, the interactions between the two teams tend to be reactive: the problems encountered by the red team return to yellow, which seeks to solve them.

The implementation of an orange team, however, presupposes a more proactive attitude on the part of developers. By learning from the red team about vulnerabilities that can be avoided at the code level, fewer problems will be detected by "authorized hackers" and, consequently, less time will be spent by both teams.

Green Team - This team is about communication between the yellow and blue teams. Its goal is to improve code-based defenses and application design. This happens through the feedback of the blue team regarding the application and the sharing of limitations of the software by the yellow team. These interactions help identify vulnerabilities and build defense strategies early in the application development cycle.

White Team - The white team is responsible for maintaining the security standards required by internal and external auditors (PCI, ISO 27001, among others) and for the policies and requirements of the business. This is a neutral team that organizes the other, plans and monitors their progress.

Why implement?

Information security teams are a way to organize security procedures and implement them throughout the software development cycle, rather than just at the end.

Risk Management Methodologies

Risk management is a process that aims toenable the effective security of systems, responsible for processing, storage and transmission of information; it creates a solid basis for decision making, especially in relation to coherent budget execution and investment in technologies necessary to mitigate impact risks for the company.

I. Reactive and Proactive Approach

When a particular security incident occurs, many IT professionals tend to act to contain the situation, discover the causes, and repair the damage in the shortest possible time. Such an approach is said to be reactive, it depends on a stimulus caused by an incident for actions to be taken.

Responses to incidents are tactically effective, especially if performed rigorously to discover the root causes. As a result, recent security incidents may assist in preventing futureincidents.

The proactive approach to managing security risks aims to reduce the probability of an incident with the use of control plans. Unlike the approach, the proactive approach does not wait for an incident toarise.

II. Vulnerability Identification

Vulnerabilities are flaws or weaknesses in security processes, projects, development, or internal controls of a system, which, if exploited, can result in unwanted events, that is, attacks. Proactive testing methods can be used to identify vulnerabilities:

- Scanning and vulnerability analysis systems;
- Tests and simulations;
- System intrusion tests;
- Audits in source codes;
- Security-critical checklists and analysis.

Conclusion

Information Security is much more than having antivirus software installed or using a firewall that prevents undue agents from attacking your network. Information Security is related to data protection, physical security, environmental security, the alignment of Information Technology with the objectives and mission of the company, among other functions essential for business continuity. Therefore, its fundamental in the current scenario in which we are, not only as a reactive measure, but with organized planning and proactive measures.