Scientific and Practical Cyber Security Journal (SPCSJ) 4(2): 59-62 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

RECOMMENDATIONS TO THE SELECTION OF STAKEHOLDERS FOR THE PROTECTION OF CORPORATE INFORMATION AND TELECOMMUNICATIONS SYSTEMS

[1] Osadcha Olha, [2]Vialkova Vira[1-2] Faculty of Information Technology
Taras Shevchenko National University of Kyiv, Ukraine

ANNOTATION. With Next-Generation Firewall (NGFW), businesses can quickly create security policies that comply with business policies, are easy to maintain, and adapt to a dynamic enterprise environment. They reduce response time through automated policy-based actions, while the IT department is able to quickly automate workflows by integrating with administration tools.

KEYWORDS: *next generation firewall, next generation firewall, next-generation firewall, NGFW, policy, ITS, information security management, cybersecurity, threats, network, protection, administration, attacks.*

INTRODUCTION

The main problem of information security management is insufficient funding of this area by organizations, both public and private. If we talk about direct management, employees who have already studied in the field of information security management (as a managerial function) or management of technical means of security at the university begin to work in the direction and successfully use their skills in relevant positions in business or government.

In this report, I want to consider how, with sufficient funding, a competent manager and technician can improve the situation of a private or public enterprise with the help of technical means of information protection.

FORMULATION OF THE PROBLEM

The relevance of the topic is that such organizations are evolving and need protection, so face the following problems:

- increase in information risks due to the emergence of modern threats to information systems;
- free access of personal computers to global resources leads to the dissemination of confidential information;
- a significant increase in the amount of information resources that are accumulated, stored and processed by computers and computers. According to various estimates, today about 90% of the information capital of all existing enterprises is stored in digital form;
- rapid modernization of information systems, which has become a catalyst for the emergence of new threats to information resources. Modern software due to competition and the desire of companies to continuously increase profits enter the market with shortcomings and vulnerabilities.

PROTECTION OF INFORMATION AND TELECOMMUNICATION SYSTEM OF THE ENTERPRISE

If we talk about the functional area, it is at this time that there are problems in choosing the technical means. The information security market offers a wide range of both software and hardware products. In this report, we will consider the next-generation firewall as a universal means of enterprise protection.

Let's analyze the main factors in choosing the products of the next generation of firewalls:

1. The highest priority of the firewall is to prevent attacks and ensure the security of the company. Therefore, the product must have the following capabilities:
    - blocking threats before they enter the network;
    - high-quality next-generation IPS system integrated into the firewall in order to detect hidden threats and quickly neutralize them;
    - filtering URLs to enforce policies on hundreds of millions of URLs;
    - built-in "sandbox" and advanced protection against malware, which continuously analyzes the behavior of files for quick detection and elimination of threats;
    - own anti-virus analytics department, which conducts global threat research and provides NGFW firewalls with the latest updates to prevent emerging threats.
2. Full visibility of events in the network. Your firewall should provide a holistic view of network activity that allows you to evaluate:
    - activity threats to users, hosts, networks and forced downtime;where and when the threat occurred, where else it was in your extended network and what the situation is now;активні програми та веб-сайти;
    - communication between virtual machines, file transfer and more.
3. Flexible management and deployment capabilities. No matter what the size of the business - small, medium or large enterprise - the firewall must meet the specific requirements of our company. On-Demand Management - Choose from the NGFW's built-in "manager" or centralized management system for all devices. Deployment option - locally or in a virtualization system using a virtual firewall. Customize features to suit your needs - just get new subscriptions to get more features.
4. Fast detection time. The next generation firewall should be able to:
    - detect threats in seconds;
    - determine the presence of a successful break within a few hours or minutes;
    - prioritize reports of attacks so that a specialist or IS can quickly and accurately address threats.
5. Integrated security architecture provides automation and reduces the complexity of administration. The next-generation firewall should not be an isolated tool: it should share information and work with other components of the security architecture. Therefore, choose a product that meets the following requirements:
    - easily integrates with other tools from the same manufacturer;
    - automatically exchanges data on threats, events, policies and contextual information with email security tools, endpoints and network components;
    - automates security tasks such as impact assessment, policy setting, and user identification.

    Firewall helps to universally protect data of any type of organization.

    According to Gartner analysts, next-generation firewalls are guaranteed to provide the following:
    - protection against continuous attacks by infected systems;
    - standard features for the first generation of firewalls;
    - IPS-based application type signatures;
    - traffic inspection, including applications, as well as detailed and customizable control at the application level;
    - the ability to include information outside the firewall (for example, integration with network directories, "white" and "black" lists of applications);
    - the ability to constantly update databases and applications and threats;
    - inspection of SSL-encrypted traffic.

The main task is the correct configuration , constant monitoring by the technical staff. In this case, the firewall can prevent most problems.

USING THE SANDBOX MECHANISM FOR ADDITIONAL ITS PROTECTION

Modern cyberattacks are increasingly targeted at a specific industry or a specific company. The unique nature of such threats allows you to easily bypass the classic means of protection - antivirus, firewalls, IPS, mail and web gateways, etc. The ultimate goal of the attackers - to transfer money in their favor, to commit espionage, theft of valuable information, extortion, stop production and disable equipment.

Means of detecting modern attacks, such as sandboxes, as well as preventive measures (incident analysis, localization of infection in the network, actions to prevent attacks and prevent recurrence of incidents) help to effectively neutralize targeted attacks[1-4].

Sandbox - a mechanism for safe execution of programs. Sandboxes are often used to run unverified code from unknown sources and detect viruses and bookmarks[5-8]. In antiviral tools, simple detection methods, such as signature analysis, the presence of behavioral analysis, do not allow to detect carefully planned penetration. And the mechanism of the sandbox launches a file on a regular OS with a complete analysis of what is happening. It is launched at an isolated station under close supervision. This is especially true in cases where the malware pauses at the beginning of its work.

The known and deliberately malicious code will not go to the sandbox, because the verdict is so clear, the firewall will not miss it. Only if the firewall does not have enough data to make a decision, it sends it to the sandbox.

The sandbox can be cloudy, and can work locally in the company, the functionality does not change. The code is run, its behavior is monitored. This way you can track what is happening on the virtual machine and see what this file could do if it got on your PC.

Usually not all firewalls are able to delay the file to get a verdict from the sandbox, you need another agent on the workstation. And then you need that after the file is downloaded, the check in the sandbox is not instantaneous (the manufacturer usually guarantees around 5 minutes). In any case, the user has enough time to open this file. Often it is a set of technical solutions at different levels, which serves one task.

Manufacturers maintain specialized knowledge bases that allow you to identify more threats. There are reputational checks, in which case the reputational model is used. The necessary information gets there, and then on its basis the indicator of compromise is formed. That is, it detects a malicious file, we understand how it works, and in this case it is more efficient to send information about it to all PCs. If he accesses a file, renames it, the combination of these factors can mean an indicator of compromise, sending it to everyone, we can quickly detect vulnerabilities without resorting to the capabilities of the sandbox[9-11].

Harm testing should not be the first in the line of defense. Initially, it can be firewall, antispam, anti-phishing, which are embedded in the mail system, proxy servers, intrusion detection at the network level, and only after the file passes these barriers is the sandbox - the last resort. At this stage, it is necessary to understand that the efficiency of file verification requires large resources, a large flow of such files will incur additional costs. To reduce them, you must first make the most effective use of existing remedies.

CONCLUSION

You should be especially careful to choose equipment that protects your LAN. You need to know what set of features should be included in the device for a specific situation and company. If the company needs to meet high safety requirements, you need to choose NGFW.

Recently, the number of cyberattacks on businesses has increased significantly. In this regard, the author recommends using NGFW to protect the perimeter of the network and internal services of the company.

In addition, the use of equipment with a sandbox mechanism is recommended. With its advent, the security of many companies has risen to a new level.

REFERENCES:

1. Jithin Aby Alex, Being a firewall engineer: An operational approach: A Comprehensive guide on firewall management operations and best practices, 1st Edition, 2018.
2. Aaron Woland, Vivek Santuka, Mason Harris, Jamie Sanbower, Integrated Security Technologies and Solutions - Volume I, 1st Edition, 2018.
3. What are the advantages of next-generation firewalls? Review of popular NGFW . Access mode: https: // www.ixbt.com / live / market / v-chem-preimuschestva-fayrvolov-sleduyuschego-pokoleniya-obzor-populyarnyh-ngfw.html.

4. Site organization Gartner. Access mode: https: // www.gartner.com / en / information-technology / glossary / next-generation-firewalls-ngfws
5. 5 critical mistakes when evaluating a next-generation firewall . Access mode: https: // www.paloaltonetworks.com / content / dam / pan / en_US / assets / pdf / white-papers / five-critical-mistakes-to-avoid-when-evaluating-a-ngfw.pdf .
6. A. Gagnidze., M. Iavich., G. Iashvili, Analysis of Post Quantum Cryptography use in Practice, Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 2, 2017, p.29-36.
7. A. Gagnidze, M. Iavich, G. Iashvili// Novel Version of Merkle Cryptosystem, BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES, vol. 11, no. 4, 2017, p. 28-33
8. NGFW or UTM: How to Choose. Access mode: https: // www.watchguard.com / en / wgrd-resource-center / help-me-choose
9. 5 Tips for Choosing a Next-Generation Firewall. Access mode: https: // www.cisco.com / c / dam / en / us / products / collateral / security / next-gen-firewall.pdf.
10. Overview of programs for working with virtual sandboxes . Access mode: https: // www.ixbt.com / soft / sandboxes.shtml
11. Гагнидзе А.Г., Явич М.П., Иашвили Г.Ю. Пост-квантовые криптосистемы // Современные научные исследования и инновации. 2016. № 5 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2016/05/67264