UDC 621.396

INFORMATION SECURITY REQUIREMENTS FOR A SMALL BUSINESS COMPANY

LIANG JINHUI, N.V. NASONOVA

Belarusian State University of Informatics and Radioelectronics, Republic of Belarus

Submitted 8 November 2020

Abstract. The most common types of threats, as well as attacks and intrusion methods were analyzed. Adaptive Security Architecture model was used to effectively mitigate the considered threats. Using the information classes and its characteristics, information security requirements have been developed for storing and processing critical information in the network of a small business.

Keywords: information security attacks and intrusions, information security requirements, small business companies.

Introduction

The number of external attacks on the infrastructure of organizations is growing significantly. This problem is especially relevant now, when many companies are in a hurry to transfer employees to remote work. Hackers look for any open breach in systems at the perimeter of the network, for example, a forgotten unsecured web application, not updated software, or an incorrectly configured server with a weak administrator password. The larger the compromised company and the higher the privileges obtained, the more profitable the transaction can be made by the criminal.

The legal definition of «small business» is not strictly fixed and varies by country and by industry. Commonly it depends on a number of employees, annual sales, value of assets and net profit, alone or as a combination of factors. In most of the countries the number of employees in a small business company is assumed up to 50–250 persons.

Relevance of information security for a small business company

It is widely believed that the problem of cyberattacks by low-skilled hackers (the so-called script kiddies) is more relevant for small companies that are not ready to invest heavily in protecting their resources. Large organizations invest much more in information security and, it would seem, should be better protected. But penetration testing demonstrates the vulnerability of even large companies. Refer to the statistics collected by Positive technologies for 2019 [1]. Information about the most common types of threats, as well as attacks and intrusion methods based on the analysis of statistics, is presented in the table.

Suspicious network activity was detected in the infrastructure of 97 % of companies. In 28 % of companies, the activity of a number of utilities and tools was revealed, which may indicate a compromise. There is a trend towards «living off the land» attacks. Also, attempts to discredit or destroy a competitor's business led to an increase in DDoS attacks. In 81 % of organizations, in-depth analysis of network traffic revealed malware activity. Multiple attempts to connect to external servers on port 445/TCP (SMB) indicate a malware infection. But miners and adware were more common in the infrastructure. Thirty-three percent of companies use dictionary passwords, which gives rise to a large number of brute-force attacks or dictionary attacks. At the network perimeter of 11 % of companies, the main security problem is inadequate protection of web applications. Thus, after analyzing the results of the above statistics, we can conclude that the security of the corporate network, and therefore the continuity of the technological process, directly depends on the efficiency of administration of networks and network equipment, as well as the timely installation of relevant security updates for the software used. The statistics analysis results are given in Table 1.

Table 1. **Types of attacks and intrusions in corporate networks**

Categories of identified threats	Percentage of companies (%)	Intrusion methods	Types of attacks

Suspicious network activity	97	– hiding traffic;
		– network scanning;
		– attempts to remotely start the process;
		– collection of information about active network sessions on nodes, users, groups, password policy, etc.;
		– perimeter scan.
			– DDOS;
			– IP spoofing;
			– living off the land.

Violation of IS parameters	94	– use of unprotected data transfer protocols;
		– use of software for remote access;
		– using BitTorrent;
		– open network ports on the perimeter.
			– phishing;
			– mailbombing;
			– SPAM;
			– telephone phreaking;
			– pre-texting.

Malware activity	81	– miners;
		– adware;
		– spyware;
		– reading arbitrary files.
			– WannaCry;
			– worms;
			– viruses;
			– Trojan horse;
			– spyware;
			– ransomware.

Attempts to exploit software vulnerabilities	28	availability of exploits in the public access	Rootkit

Password guessing attempts	19	– using dictionary passwords;
		– saved authentication parameters;
		– obtaining and increasing privileges.
			– brute force;
			– by dictionary.

Attempts to exploit web vulnerabilities	11	– using vulnerabilities in XML and WEB services;
		– forging cross-site requests.
			– cookies infection;
			– SQL injection;
			– XSS Scripting.

When developing corporate information security systems for companies for which the cost of information leaks and other incidents may be the highest, it is necessary to rely on existing standards that have already proven themselves in this area of working with data and combating cybersecurity threats. In a narrower sense, the Adaptive Security Architecture (ASA) model, first introduced to the market in 2014 [2], will be a successful solution. Within the framework of this model, protection against targeted attacks is prioritized, but at the same time it provides the maximum possible defense against all internal and external threats provided for by the security policies of a particular organization. The ASA model assumes building a security architecture at four levels [3]:

– prediction (forecasting);

– warning (prevention);

– identification (detection) of threats;

– response.

First of all, when developing methods for protecting a corporate network, one should rely on the classification of data and processes circulating in the network [4, 5]. This is necessary in order to understand what exactly is to be protected and what are the priority areas of protection, since without prioritization the proper level of protection will not be achieved. It is necessary to find out which systems need to be protected in the first place, that is, those without which the organization's action will simply stop. Also, determine the systems on the protection of which you can save money or not at all. For small businesses, the following types of information circulating in the company's network can be distinguished, which are subject to protection:

– client database with important confidential data (numbers of documents, cards, details of visa services);

– information about quotas, insurance payments and policies;

– accounting software, accounting, taxes;

– individual schemes and developments for attracting clients, details of promotions and other information constituting scientific, technical and technological information related to the company's activities;

– personal data of employees of the enterprise and partners, stored in the database and transmitted over the network;

– e-mail messages and database information containing service information, information about the activities of the enterprise, etc.

The assignment of security categories to an information network is based on an assessment of the damage that can be caused by security breaches. There are three main aspects of information security: availability, confidentiality, and integrity. IS violations can affect only a part of these aspects, just as safety regulators can be specific for certain aspects. Therefore, it is advisable to assess the possible damage separately for violations of accessibility, confidentiality and integrity, and if necessary, an integral assessment can be obtained. When categorizing an information system, the categories of information stored, processed and transmitted by means of IS are taken into account, as well as the value of the assets of the IS itself in accordance with the scale (Table 2) [5].

Table 2. **Types of attacks and intrusions in corporate networks**

Damage level	An impact, produced by loss of availability, confidentiality and / or integrity on the organization's operations, assets and people	Impact to the company's business
High	a severe or catastrophic impact	the company loses the ability to perform all or some of its main functions
Moderate	a serious detrimental impact	the company remains able to fulfill the mission assigned to it, but the effectiveness of the main functions is significantly reduced
Low	a limited detrimental impact	the company remains capable of fulfilling the mission entrusted to it, but the effectiveness of the main functions is significantly reduced

Thus, in most commercial private small businesses, the following categories of confidential information can be distinguished:

– personal data;

– commercial information.

The most important aspect of the information security policy of any company is ensuring the security of personal data. The security of personal data is achieved by eliminating unauthorized, including accidental, access to personal data, which may result in the destruction, modification, blocking, copying, distribution of personal data, as well as other unauthorized actions. Statistics have shown that the largest number of threats observed in 2019 is associated with suspicious network activity detected in 97 % of organizations, which leads to the collection of information about active network sessions on nodes, about users, groups, password policies, etc. This includes an increase in the number of social engineering methods, respectively, an increase in such attacks as phishing, telephone phreaking, pre-texting, etc. Accordingly, these types of threats can lead to a violation of the confidentiality and availability of stored confidential information, including personal data [4].

Therefore, the following information security requirements have been developed for storing and processing confidential information in the network of a small business:

– information and related resources must be available to authorized users;

– differentiation of access of registered users to hardware, software and information resources of the network (the ability to access only those resources and perform only those operations with them that are necessary for specific users to perform their official duties);

– registration of user actions when using protected resources in system logs and periodic control of the correctness of system users by analyzing the contents of these logs;

– protection of personal data from leakage through technical channels;

– protection of personal data from unauthorized disclosure;

– compliance with the procedure for storing personal data on paper and electronic media;

– development of regulations for responding to incidents and related procedures;

– protection against unauthorized modification and control of the integrity of the software used in the network, as well as protection of the system from the introduction of unauthorized programs;

– implementation of mechanisms for automatic blocking of detected malware by removing them from program modules or destroying them;

– checking the integrity of anti-malware protection modules required for its correct functioning;

– availability of means for restoring the personal data protection system;

– allocation of a communication channel that ensures the protection of personal data;

– exchange of personal data, during their processing in the information system, through communication channels, the protection of which must be ensured by the implementation of appropriate organizational measures and (or) the use of technical means;

– restriction of unauthorized outgoing traffic from applications used to process, store or transmit confidential information and personal data;

– the use of strong encryption to protect confidential information and personal data, transmission or remote access to which is carried out using mobile and portable devices that support network authentication.

Conclusion

97 % of organizations reveal suspicious network and malware activity. Adaptive security architecture helps businesses stay ahead of cybercriminals, suggests flexible security measures to protect data and systems in as agile a way as possible, rather than relying on outdated perimeter defense strategies. Using the information classes and its characteristics, information security requirements have been developed for storing and processing critical information in the network of a small business.

References

1. Current Cyber Threats: Results of 2019 [Electronic source]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/.

2. What is Adaptive Security Architecture? [Electronic source]. URL: https://adaptivesecurityarchitecture247.wordpress.com/2016/04/16/what-is-adaptive-security-architecture-2/

3. Weise J. Designing an Adaptive Security Architecture. Sun BluePrints Online, 2008.

4. Top Cybersecurity Threats in 2020 [Electronic source]. URL: https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

5. Vacca J.R. Computer and Information Security Handbook. Morgan Kaufmann, 2017.