БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ • BULGARIAN ACADEMY OF SCIENCES

ПРОБЛЕМИ НА ТЕХНИЧЕСКАТА КИБЕРНЕТИКА И РОБОТИКАТА, **71**
PROBLEMS OF ENGINEERING CYBERNETICS AND ROBOTICS, **71**

София • 2019 • Sofia

Security Policies for Wireless and Network Infrastructure

Georgy Kostadinov, Tatiana Atanasova

Institute of Information and Communication Technologies 1113 Sofia
Emails: ***g.kostadinov@iit.bas.bg***, ***atanasova@iit.bas.bg***

Abstract: *The security is the main element of every data network. Security must be integrated into the design of the network and provide the three basic requirements for data transmission - authenticity, integrity, confidentiality. The paper presents requirements for the network security provision. General network security methods are provided. Special attention is paid to wireless network security.*

Keywords: *security, security methods, network infrastructure, wireless networks*

1. Introduction

Security policies are one of the most important controls in any organization. These controls include network security and describe the specific technology, hardware or software that will be used, as well as the acceptable and unacceptable use of the organization's assets.

The network security is based on regulations and internal organizational policies adopted by the organization and implemented and monitored by its network experts and administrators as prevention of unauthorized access, misuse of data or configurations, as well as monitoring and recording of such events. All of these may result in denial of service or network resources, unauthorized access, and theft or loss of data. Policies should be applied across the organization consistently and give the opportunity to track the actions of users who carry out their normal activities.

For Network Security Policy there is no single mechanism for protecting the network [1, 2]. There is no one-size-fits-all network security mechanism because any security system can be compromised, if not externally, then internally.

This paper discusses the main aspects of applying the network security policies and proposes guidelines for its provision. The rest of the paper is organized as follows: Section 2 introduces network security levels; Section 3 provides methods for general network security; Section 4 considers aspects of wireless network security with some recommendations for its improving. Section 5 concludes the exposition.

2. Security levels

Network security is implemented through a set of tasks and tools that are used by the organization to protect against unauthorized access to the computer networks and related devices of people and applications. Different levels of security (layers of security) are applied to ensure network security [3], so the attacker must compromise two or more systems to gain access to assets critical to the organization.

Network security, monitoring and recovery strategies must be implemented in network security policies.

Security - All systems and networks should be configured as correctly as possible, following the latest manufacturer's recommendations and following best practices.

Monitoring – It needs to be identified at all times if there is a change in configuration or it is a network traffic that is not typical for the network or systems running on it.

Recovery - If a problem is identified, devices and systems must be restored to the latest safe state as quickly as possible.

3. General network security methods

Network security methods are described as different types of network security provision:

- **Access control** - Block unauthorized users and devices that have access to the network.
- **Malware protection -** virus, malware and trojan protection measures must be able to prevent the initial infection and be able to eradicate the malicious code after being infected.
- **Application security** - hardware, software, and processes must be used to protect against network access through unsecured applications.
- **Behaviour analysis -** the normal behaviour of the network must be known and documented in order to detect anomalies or breaks, if any.
- **Data loss prevention** - technologies and processes must be put in place to ensure that data relevant to the organization is not intentionally or unintentionally transmitted outside the organization, damaged or destroyed.
- **E-mail security** - E-mail security tools can block both incoming attacks as well as outbound information important to the organization through outgoing messages.
- **Firewalls -** network security tools that, following the rules, allow or prohibit the flow of traffic between networks internal and external to the organization by building security barriers.
- **Intrusion detection and prevention -** systems that scan network traffic to detect and block attacks by comparing network activity to databases for known hacking techniques and attacks.
- **Network segmentation** - network partitioning software classifies and segments network traffic, facilitating security policies.
- **Web security -** Internet usage in the organization and blocking of web-based threats should be controlled when using browsers as a point of entry for infecting the network.
- **Virtual private networks** (VPNs) –IPSec or SSL based tools that authenticate communication between a device and a secure network by creating an encrypted tunnel.
- **New legal provisions** (GDPR - General Data Protection Regulation in EU (European Union) [4]) **-** the organization must put in place the necessary measures and controls to protect the integrity and confidentiality of its data entrusted with regulatory requirements.

Every organization is required to establish, observe and comply with organizational policies, procedures and guidelines for:

- creating instructions with rules for installing computer systems and applications;
- creating a guide for building a local area network;
- creation of job descriptions of employees and specific instructions and regulation of their work with computer systems and electronic documents.

At last but not least it is physical security, which also uses technical security features such as: video surveillance systems, alarm systems, access control with personal magnetic cards, etc.

4. Wireless Network Security

A wireless local area network (WLAN) is a group of wireless network devices in a limited geographical area, such as an office building that exchanges data through radio communications. The security of each WLAN depends to a large extent on how well each component is secured - client devices access points (AP) and wireless switches throughout their WLAN whole lifecycle from initial design and deployment through ongoing maintenance and monitoring.

Wireless networks do not have the security features of cable networks, such as firewalls, intrusion prevention systems, content filters, and malware detection programs. Thus the open communications environment makes wireless transmissions more vulnerable than wired communications to malicious attack [5].

Wireless networks provide wireless access points that may be susceptible to infiltration. The lack of all security available on cable networks makes them susceptible and vulnerable to attacks designed to gain access to corporate networks.

Wireless security protocols are constantly evolving [6] to compensate for the continued development of wireless network attack types. For example, the protocol WPA3 (Wireless Protected Access 3) includes 128-bit advanced encryption according to the AES standard.

All organizations must follow and apply good practices to protect their enterprise wireless networks:

- implementation of a wireless intrusion detection and prevention system;
- software and firmware update monitoring of all wireless devices and components as recommended by the manufacturer;
- reliable device configuration according to the organization's security policies, manufacturer's recommendations, and best practices;

- implementation of multifactor authentication - an additional factor of authentication - such as active directory or server radius (RADIUS);
- splitting the wireless network for employees and guests by segmenting traffic and different network identifiers – SSID.

Several recommendations for improving security in wireless networks [6] are as follows:

- enter filters with MAC addresses that are allowed;
- hide network identification SSID;
- reducing the signal strength of the radiating access points so that they cover only the areas for which they are intended;
- periodic scanning for vulnerability (Vulnerability Scans), both inside and outside, comparing results from previous scans;
- end-to-end traffic encryption on the level of application layer using techniques such as SSL or SSH.

The number of different types of attack, and the many possible solutions, makes it a difficult task to put in place an appropriate wireless network security policy. Such a policy must address both the size and nature of the enterprise, and the resources available to it [7].

5. Conclusion

The technology is increasingly developing, so the need of tools to ensure that the networks are better protected is extremely welcomed. The Internet of Things (IoT) and Machine-to Machine (M2M) are fast growing examples of the network technology development. IoT connects many different physical devices that collect and share data via wireless networks to the Internet. The data can be extremely sensitive. So the security is one the biggest issues with the IoT [8]. The importance of network security policies should not be neglected. Extensive research efforts have been devoted to the security issues in wireless networks, but numerous challenges still remain open.

References

1. Tipton H. F., Krause M., Information Security Management Handbook, Fifth Edition, CRC Press, Dec 30, 2003 - Computers - 2036 pages.
2. What Is Network Security? https://www.cisco.com/c/en/us/products/security/what-is-network-security.html#~types-of-network-security, accessed January 2020.
3. Rexha B., Qerimi E., Neziri V., Dervishi R. Using eID Pseudonymity and Anonymity for Strengthening User Freedom in Internet, CEEE|Gov Days 2015, National University of Public Service, Budapest, Hungary, Vol. 1, p.1-9.

4. Hristov, P., Dimitrov, W. The blockchain as a backbone of GDPR compliant frameworks. – Proceedings of 8th International Multidisciplinary Symposium - Challenges and Opportunities For Sustainable Development Through Quality and Innovation in Engineering and Research Management, Vol. 20, 2019, No 1, p. 305-310.
5. Zou, Y., Zhu, J., Wang, X., Hanzo, L., A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends, Proceedings of the IEEE, 104(9),7467419, 2016, p. 1727-1765.
6. Alexandrov, A., Monov, V. Method for WSN clock synchronization based on optimized SLTP protocol. Proceedings of IEEE 25 Telecommunications Forum TELFOR 2017, p. 139-142.
7. WoodwardA., Recommendations for wireless network security policy: an analysis and classification of current and emerging threats and solutions for different organisations, 2005, Proceedings of 3rd Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia
8. Dineva, K., Atanasova, T., Security in IoT Systems, Proceedings 19th International Multidisciplinary Scientific Geoconference SGEM 2019, Vol. 19, Informatics, Geoinformatics and Remote Sensing, Issue 2.1, 2019, p. 576-577.

Acknowledgments: This paper is partially supported by the Bulgarian Ministry of Education and Science (contract D01–205/23.11.2018) under the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICT in SES)".

Политики безопасности для беспроводной и сетевой инфраструктуры

Георги Костадинов, Татяна Атанасова

Институт информационных и коммуникационных технологий, 1113 Sofia
Emails: ***g.kostadinov@iit.bas.bg, atanasova@iit.bas.bg***

Аннотация: *Безопасность является основным элементом любой сети передачи данных. Безопасность должна быть интегрирована при проектировании сети и обеспечивать три основных требования для передачи данных - подлинность, целостность, конфиденциальность. В статье представлены требования к обеспечению безопасности сети. Разгледаны общие методы безопасности сети. Особое внимание уделяется безопасности беспроводных сетей.*

Ключевые слова: *безопасность, методы безопасности, сетевая инфраструктура, беспроводные сети*