UDC 004.056.5

AUDIT OF INFORMATION SECURITY OF TELECOMMUNICATION NETWORKS OF CREDIT AND FINANCIAL INSTITUTIONS

S.N. PETROV, A.M.E. ELBUAISHI, T.A. PULKO

Belarusian state university of informatics and radioelectronics, Republic of Belarus

Submitted 20 November 2018

Abstract. The urgency of the audit of credit and financial institutions telecommunication networks conducting, associated with the increase of the network infrastructure load and the increase of the remote banking systems' users number is shown. The information security auditing standards are analyzed. The basic recommendations on networks audit conducting are presented.

Keywords: information security audit, ISO/IEC 27001, network security, credit and financial institutions, penetration test.

Introduction

Information security audit is carried out in order to determine the information system's security compliance with the standards requirements, external or internal, and also to determine the degree of protection of the information system from actual informational security threats.

There are international (ISO/IEC 27001: 2013, ISO/IEC 27005: 2010, ISO/IEC 27033, PCI DSS), as well as industry and national regulations on information security for the system of credit and financial institutions (banks). Technical control of the security of information assets is carried out using special software and hardware systems (vulnerability scanners).

In addition to bank, there are non-bank credit and financial institutions, as well as non-credit financial institutions that operate on the money market and specialize in one or more banking operations. These include leasing companies, credit unions, investment companies (funds), insurance companies, pension funds and charitable funds, collectors firms, pawnshops, trust companies, billing and clearing centers. The annual penetration testing is required from the listed above organizations, depending on the volume of committed financial transactions per day (excepting microfinance organizations, consumer credit cooperatives and pawnshops).

This sphere is characterized by widespread use of information technologies, a large number of individual clients and high attractiveness for fraudsters. It resulted in the fact that in July 2018, Central Bank of the Russian Federation made mandatory annual penetration testing [1] and analysis of information security vulnerabilities of information infrastructure facilities (for the banking sector of the Russian Federation). The application software vulnerabilities analysis will be carried out by the licensed organizations.

Thus, conducting an audit is one of the important links in the chain of information security.

Specificity of computer network security audit

The ISO/IEC 27001 certificate [2] is a prerequisite for participation in many government procurement, auctions and tenders, it provides additional benefits to certificate holders, for example, it makes possible to export software to other countries. Certification involves the following steps: preparation, certification readiness verification by experts, certification check, certificate issuance. Such work is usually performed by a third-party company with the relevant experience. Also, in order to receive a certificate, it is necessary to conduct training of the staff designated as responsible for maintaining the information security management system documentation. As a result – the high cost of certification.

In this work, the specific aspects of the ISO/IEC 27001 standard connected with network security audits, as well as the tools for conducting technical controls will be considered

In the ISO/IEC 27001 standard there are 4 information security objectives, interconnected in data networks:

Access control. Users should only access those networks and network services where they have authorization for.

Physical security and protection from natural threats. Cable protection. Supply cables, transmitting data cables or ensuring the information services operation cables should be protected from interception, interference or damage.

Information sharing security. Networks must be managed and monitored to protect information in systems and applications. Security mechanisms, service levels and management requirements should be defined for all network services and included in network maintenance agreements. Different groups of information services, users and information systems should be separated in networks. The information transmitted by electronic communications must be adequately protected.

Acquisition, development and maintenance of systems. Information used by application services transmitted over public networks should be protected from fraudulent activities, claims connected with the breach of contractual obligations, and unauthorized disclosure and modification.

Today, data is transmitted through the internal networks of banks, mail and file systems, videoconferencing systems and automated banking systems, enterprise resource management systems and customer relationship management. External networks connect banks to data centers, outsourced contact centers, SWIFT networks, etc. There has been a steady increase in the number of users of mobile and Internet banking. For example, according to statistics from the National Bank of the Republic of Belarus [3], an increasing number of Belarusians prefer to use Internet banking (3.41 million users) and mobile banking (1,22 million) to make payments and transactions (Fig. 1).

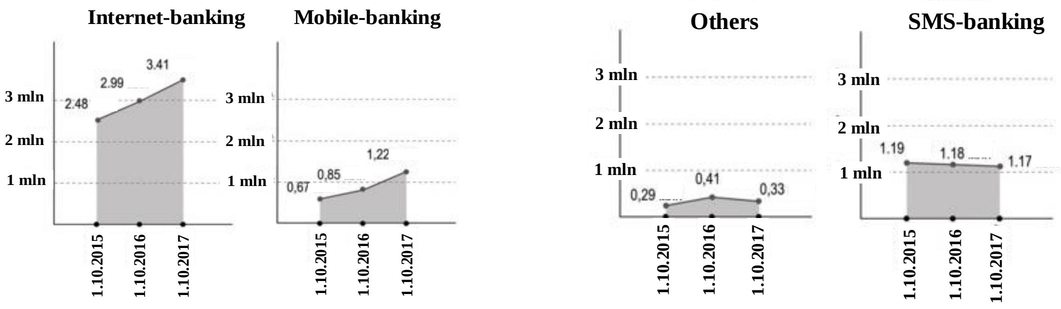

Fig. 1. Trends in using remote banking channels

The instrumental study of the network infrastructure is carried out by using software and hardware and software security analysis: security scanners, integrity monitoring systems, code analysis systems, distributions of pentest. To simplify the analysis, it is necessary to carry out a detailed elaboration, that is a division of the network structure into its constituent elements. There are several network segments, such as the demilitarized zone, local VPN-pool address, external addressing segments, closed segments (for example, bank-client segments, automated workstations of operators, videoanalytics, billing).

To conduct a perimeter inventory for the selected segments, that includes checking the methods and channels of Internet access, used external addresses, systems available from the Internet, services and protocols, authentication methods.

Conclusion

The information security audit is an effective tool to obtain the objective assessment of the current level of protection of a credit and financial institution from various informational threats. Improving the audit process will allow to increase the level of information security. The detailed description of the company's network infrastructure is one of the key aspects of the computer and telecommunication networks audit.

References

1. Proekt popravok v Polozhenie Banka Rossii № 382-P «O trebovanijah k obespecheniju zashhity informacii pri osushhestvlenii perevodov denezhnyh sredstv i o porjadke osushhestvlenija Bankom Rossii kontrolja za sobljudeniem trebovanij k obespecheniju zashhity informacii pri osushhestvlenii perevodov denezhnyh sredstv». [Electronic resource]. URL: http://regulation.gov.ru/Files/GetFile?fileid=c9178fad-6c64-4eb7-9c57-43b1a8528a5b (date of access: 22.10.2018).

2. ISO/IEC 27001:2013 Informacionnye tehnologii - Metody zashhity - Sistemy menedzhmenta informacionnoj bezopasnosti – Trebovanija. [Electronic resource]. URL: http://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf (date of access: 22.10.2018).

3. O populjarnyh kanalah i budushhem DBO. [Electronic resource]. URL: https://dev.by/news/o-populyarnyh-kanalah-i-buduschem-dbo (date of access: 22.10.2018).