

УДК 314.8

Michael Shapovalov¹, Yuliya Sobol²

¹ student of group RT-810, National University «Zaporizhzhia Polytechnic»

² PhD (Philology), assistant prof. National University «Zaporizhzhia Polytechnic»

INTERNET VULNERABILITIES OF LARGE ORGABIZATIONS

Nearly all organizations depend on the Internet for their vital information and communications needs, as well as for their day-to-day business operations. Thus, Internet connections are very important.

According to statistics, 7 out of 10 industrial companies are potentially vulnerable to hacker attacks. The Positive Technologies analytical group, which studied the main directions of attacks on key corporate systems of industrial organizations, confirmed that the main danger lies in weakly protected administrative channels.

The research found that cybercriminals are able to overcome the barrier through remote access to the network of an industrial organization - the number of such potentially vulnerable enterprises in the course of the research was 73%.

The reason why such vulnerabilities are present in enterprises is a banal unwillingness to change something that seems to have been working properly for a long time (fear of harming the organization's technological process). Such companies spend their main efforts on preventing the use of internal technological systems, separating local technological networks from corporate ones, which can be accessed from an open Internet network.

Administrative methods of control remain one of the main methods of gaining access to a corporate LAN - it is not uncommon for IT specialists of industrial enterprises to provide themselves with remote control for the sake of convenience, sometimes neglecting security measures.

According to the study, the most vulnerable spots of enterprise networks are passwords that can be easily found in a dictionary, as well as outdated software. By the way, these shortcomings were found in each of the companies considered.

Thanks to such errors, the attack direction can be developed to gain the highest rights of the corporate domain, as a result of which an attacker can even take control of the entire internal infrastructure.

When hackers break into a corporate network, they often use bugs in applications and corporate sites as a hacking method. Phishing is also very common (emails with hidden malicious code that hackers send to corporate addresses).

To attack the networks of large industrial enterprises, hackers often consider the ICS(Industrial control system) of equipment as a weak point, because such software uses highly specialized software and its own protocols, which are poorly protected from this type of attack.

To prevent hacker attacks on corporate networks of enterprises, necessary:

1. Reconsider the vision of the security organization, and at the highest level. Often, problems arise precisely because of the refusal of the company's management to finance funds for information security. It is necessary to develop audit regulations, conduct penetration checks, implement protective measures (systems for detecting and countering attacks; methods of processing and interconnecting events; antivirus systems; security monitoring tools, software downloads, etc.).

2. Dividing the network into segments so that hackers cannot attack critical areas, and in the event of an attempt to penetrate inside, it would be possible to identify an attack and effectively resist it at an early stage of hacking.

3. Close attention should be paid to the separation of access rights and information exchange between the office and technological sections of the corporate network. In addition, it is essential to update the software versions used at the enterprise (for example, you need to promptly update operating systems, application software, security programs, firmware of equipment).

It is very important for industrial companies to change the approach to network control and protection from outside hacker attacks. This requires identifying the current list of possible threats, understanding potential risks, identifying the most effective methods of protection and informing staff about the rules and regulations in the field of information security, delivering information about new types of threats.