INFORMATION SECURITY TOOLS IN ELECTRONIC TECHNOLOGIES

Voitkus I.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus
Andreeva O.V. - senior lecturer of the department of foreign languages

Annotation. Over the past two years, the number of investigations into information security incidents has significantly increased. The idea of information security tools is becoming more relevant every year. The most popular ones are antivirus software, network traffic analysis, new generation firewalls, web application firewall and other. For a stable and secure existence of the company, it is necessary to ensure the information security.

Keywords: information security tools, cyber-attack, software, hardware, protection.

Introduction. Over the past two years, the number of investigations into information security incidents has increased significantly. According to the results of research by Positive Technologies, an independent high-growth global cybersecurity company consisted of ten offices on four continents, the Incident Response team detected an increase in incidents by 76% compared to 2022. Most of the attacks were targeted on IT companies, government agencies and industrial enterprises and have made up 69% [1]. It should be noted that it was Advanced Persistent Threat (APT) groups that undertook targeted prolonged cyber strikes of increased complexity and carried out 40% of the attacks. The rest was not found out at the time of the investigations. The number of incidents caused by attacks of the trusted relationships type doubled in 2023 compared to 2022 [1].

That is why the idea of information security tools is becoming more relevant every year. Information security tools are software or hardware protecting data and systems from cyber threats. There are some of them to observe.

Main part. Antivirus Software is well-known protection tool used by companies and ordinary users as well. Antivirus software, also known as computer protection software, is set of programs created to search, identify, prevent, and delete viruses that could potentially damage the system. Antivirus software can protect users against threats such as malware (worms, trojans, ransomware, spyware, adware and others), spam (inappropriate messages sent over the internet, typically to a large number of users, for a variety of purposes), phishing (a type of cyber-attack using email, phone calls, text messages, or even social media platforms). The most popular are Kaspersky Anti-Virus, Norton 360, Bitdefender Antivirus Plus 2020 and Avast Software Premium Security [2].

Network Traffic Analysis (NTA) analyzes all devices that make up the network such as routers, switches, and firewalls to determine what «normal» behavior of these devices. The main tasks are monitoring compliance with information security regulations (for example, open accounts, unencrypted mail messages), detecting attacks on the perimeter and in the infrastructure (detailed analysis of protocols), proactive threat search (to test hypotheses about the presence of hackers on the network, and to identify even hidden threats that are not detected by standard cybersecurity tools) [3].

New generation firewalls (NGFW) differ fundamentally from traditional firewalls. NGFW checks packets that go beyond ports and protocols. It is capable of filtering packages based on applications. The new generation firewall checks the package's ownership and blocks application traffic. NGFW does everything that a regular firewall: packet filtering, stateful checking, encrypted VPN traffic. But also, it can prevent more complex and evolving security threats, such as malware attacks, external threats, pre-intrusion, restricting access to suspicious sites. In general this is an inexpensive option to protect companies that want to improve their basic security [4].

Web Application Firewall is a firewall for web applications. WAF can be installed on a physical or virtual server and detects a wide variety of types of attacks. Web Application Firewall (WAF) are different from NGFW and intrusion prevention systems (IPS). WAF protects every single application from attacks. Choice of a firewall depends on the purpose and scope of the tasks. For example, the firewall called «TrustAccess» can divide the local network into segments to protect information, and delimit access to information systems at the network level. «The continent» combines several branches of an organization into a virtual private network and organize secure remote access to a corporate network [5].

Security Information and Event Management (SIEM) can monitor, analyze warnings about security breaches and immediately respond to threats. It minimizes the possible damage to business from cyber-attacks. SIEM is actively used in the investigation of information security incidents. The principle of operation is that SIEM collects information from many sources and is analyzed according to pre-established criteria. Information is taken from antiviruses, authorization and authentication systems, network equipment logs, intrusion detection and prevention programs, and others. Such system simultaneously solves many tasks: collecting, keeping, analyzing of information security events, inventory, asset analysis, control of information resource protection, monitoring of the entire IT infrastructure and reporting. Nowadays, there are several such systems, the most reputed are MaxPatrol SIEM, a popular Russian development with Russian-language technical support and documentation, certificated by the FSTEC and the Ministry of Defense of the Russian Federation and LogRhythm, issued by an American company.

Privileged Access Management (PAM) helps organization to control that each employee has only one level of access to the company's information system he needs. A privileged account is a user account with elevated privileges. It possesses permissions and access rights to the organization's systems, databases, applications and network infrastructure that most other users do not have, for example, root on Unix or Administrator on Windows. Such privileged users' actions can provoke information security risks in the case of their accounts compromise. Attackers who have gained access to the administrator's account are able to cause much more damage than when hacking an ordinary account. Another potential cyber threat is intentional malicious actions. How does it all work? Each user of the information system is given his personal account in the system, which the necessary access rights are assigned for. PAM systems are also actively used to record working hours, analyze work efficiency, and determine the resources spent. These systems manage passwords, store them in a secure database, generate and update them in accordance with security policies.

Gartner, an American research and consulting company specializing in information technology markets, released a report noting that Privileged Access Management tools can be divided into four types according to their functionality:

– Privileged Account and Session Management (PASM) – «classic» PAM functions, often enriched with password management and remote privileged access capabilities;

– Privilege Elevation and Delegation Management (PDM) – solutions that grant privileges to users within a single host;

– Secrets Management – tools for managing the lifecycle of passwords, SSH keys, one-time tokens and other secret codes;

– Cloud Infrastructure Entitlement Management (SIEM) services provide user identification and management of access rights in the cloud environment, as well as the detection of anomalies in the rights of cloud accounts and the implementation of a minimum privilege policy.

Vulnerability Management (VM) represents software applications or platforms that help organizations identify, evaluate, prioritize, and fix vulnerabilities in their networks, systems, applications, and software. A continuous, cyclical process of identifying and eliminating vulnerabilities in the organization's infrastructure and consists of the following stages: inventory of assets, identification of vulnerabilities, development of recommendations, elimination of vulnerabilities, control of vulnerability elimination.

Conclusion. For a stable and secure existence of the company, it is necessary to ensure the security of information. The choice of tools depends on the scale of the company. It is also important to use basic protection tools for ordinary users.

References

1. Results of investigations into information security incidents in 2021–2023:[Electronic resource].–URL: https://www.ptsecurity.com/ru-ru/research/analytics/outcomes-of-IS-incident-investigations-in-2021-2023-years/

2. What is Antivirus Software?: [Electronic resource].– URL: https://www.geeksforgeeks.org/what-is-antivirus-software/

3. What Is Network Traffic Analysis?: [Electronic resource]. – URL: https://www.cisco.com/c/en/us/products/security/what-is-network-traffic-analysis.html

4. NGFW: [Electronic resource]. – URL: https://cloudnetworks.ru/inf-bezopasnost/ngfw/

5. Web Application Firewall: [Electronic resource]. – URL: https://habr.com/ru/companies/beeline/articles/528258/