CYBERSECURITY: THREATS, CHALLENGES, SOLUTIONS

Atakulov Bekzod
Tashkent State Law University 12.00.09-criminal proceedings.
Applicant for independent research (PhD)in the specialty of criminology,
operational-search law and forensic science

ABSTRACT

Reliable and secure operation of data networks, computer systems and mobile devices is the most important condition for the functioning of the state and for maintaining economic stability. The safe operation of key information systems in common use is influenced by many factors: cyberattacks, disorders caused by physical impact, failure of hardware and software, humane mistakes. These events demonstrate how modern society depends on stability of information systems.

Keywords: Network, cybersecurity, information security, threats.

Cybersecurity is increasingly viewed as a strategic problem of the state, comprehensively affecting the country's economy, including the interaction of national software developers and control systems, manufacturers of equipment and components for providing ICT infrastructure, whose low market competitiveness leads to the need to use solutions from foreign manufacturers. In practice, this phenomenon leads to a rapid increase in dependence on foreign manufacturers and a decrease in the level of information protection due to the forced use of "closed" software and hardware in all segments of the infrastructure for both special government departments and the civil sector.

In the near future, dependence on foreign hardware manufacturers and software developers may reach a critical level. For example, despite the virtual "iron curtain" created, the Chinese authorities actually recognized complete dependence and insecurity due to the widespread use of the software platform for Android mobile devices (the platform's share in the Chinese market at the end of 2012 was 86.4%), based on "open" code, but controlled by US special services. From the point of From the point of view of the economy, this phenomenon has a positive impact on the development of the electronic industry and the real sector using "open" software for the production of mobile devices, but at the same time creates a real threat to national security, putting it under the control of foreign intelligence services [1].

In order for national cybersecurity to match the level of the leading economic powers, consistent actions on the part of the state are necessary, among other things, aimed at

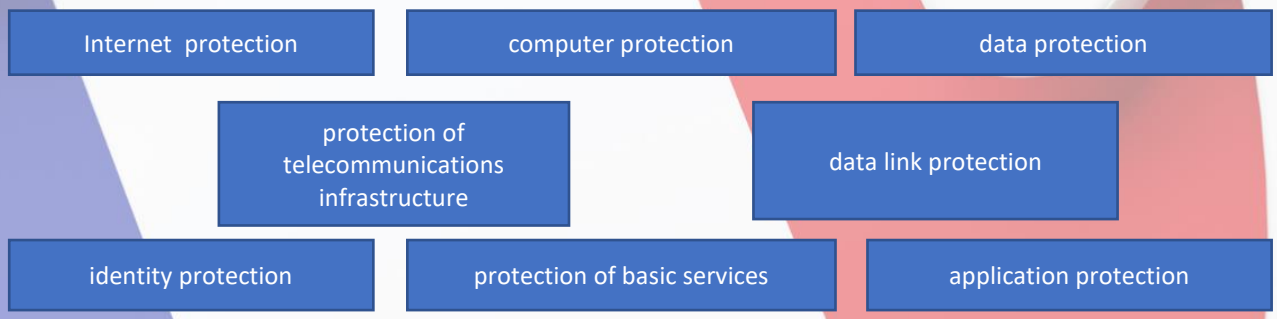
improving the efficiency and developing the system of interaction between participants in the ICT industry.

In turn, developers and manufacturers should pay special attention to the issues of information security in the developed /manufactured products, placing increased requirements on the reliability and security of the proposed solutions, and only in extreme cases and if necessary to increase the market orientation of individual products should use the solutions of foreign vendors and software developers.

Technological and systemic problems of cybersecurity

The concept of cybersecurity includes there are many problems of various types, and also contains an even greater number of solutions.

Cybersecurity is an area of active research and development in the information technology community by participants from all parts of the ICT ecosystem. Schematically, the concept of "cybersecurity" is presented in Figure 1[2].

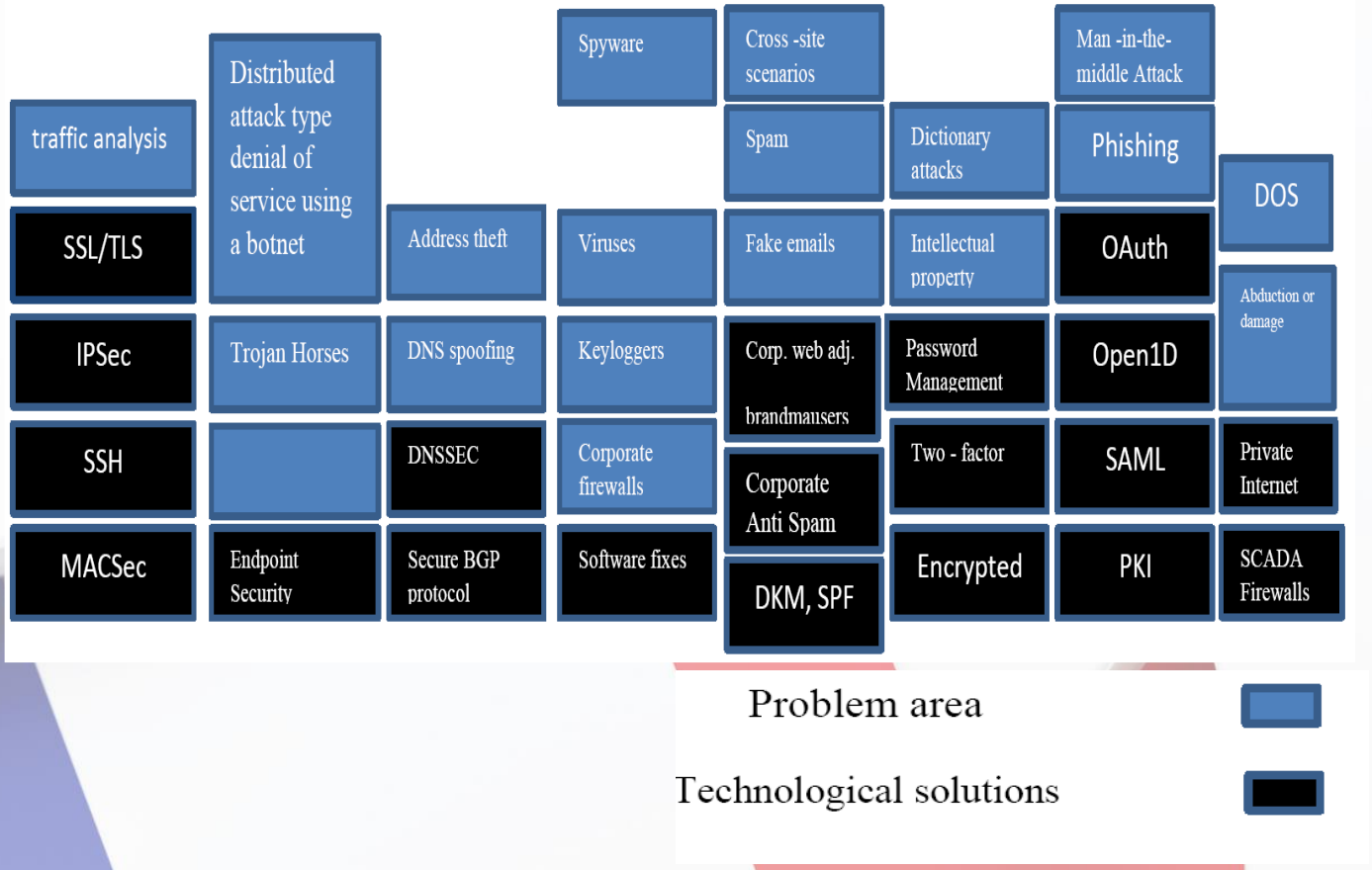


Picture. 1. Topics and directions of cybersecurity

Many areas of cybersecurity have common themes and problems that require an integrated approach.

In the vast majority of cases, the most successful attacks by hackers, criminals and other intruders are directed to end-user servers and computers connected to the Internet. Among the tools that are used to attack computers are malware, Trojan horses, botnets, phishing, distributed denial of service (DDoS) attacks, as well as man–in-the-middle attacks.

Figure 2 briefly highlights some of the areas of major cybersecurity problems, and also shows where some of these problems can be solved with the help of technical solutions developed by commercial organizations, standardization organizations and Internet users.



Pictures. 2. Cybersecurity issues and technological solutions

Ensuring cybersecurity from the point of view of engineering ownership of infrastructure

The development of cybersecurity pays special attention to infrastructure closely related to security issues. To assess the scale of the cybersecurity problem and possible threats, it is important to understand the relationship between cybersecurity, critical infrastructure (CI), critical information infrastructure (CII), protection of critical information infrastructure (CIIP) and non-critical infrastructure. Although definitions may vary slightly, critical infrastructures (CI) are generally considered to be key systems, services and functions whose malfunction or destruction has a detrimental impact on public health and safety, commercial activities and national security, or a combination of them. CI consists of both material (for example, buildings and structures) and virtual elements (for example, systems and data). Each country may have its own understanding of the term "most important", but usually this concept may include elements information and communication technologies (ICT) (including telecommunications, energy, banking, transport, public health, agriculture and food, water supply, chemical industry, shipping, as well as essential public services) [3,4].

Each of these sectors of the economy has their own material resources, such as bank buildings, power plants, trains, hospitals and government offices. At the same time, all these important sectors of the national economy depend on information and communication technologies.

Application Security-It is used to test software application vulnerabilities during development and testing, as well as to protect applications running in a production environment from threats such as network attacks, exploiting software vulnerabilities and web application attacks.

Network Security - Monitors network traffic, identifies potentially malicious traffic, and allows organizations to block, filter, or mitigate threats.

Cloud Security- Implements security measures in public, private and hybrid cloud environments by detecting and correcting false security configurations and vulnerabilities.

Endpoint Security - Deployed on end devices such as servers and employee workstations, which allows you to prevent threats such as malware, unauthorized access and exploitation of operating system and browser vulnerabilities.

Internet of Things (IoT) Security - Connected devices are often used to store sensitive data, but are usually not structurally protected. IoT security solutions help to ensure transparency and increase the security of IoT devices[5,6].

Threat Analytics - combines several channels containing data on attack signatures and threat actors, providing additional context for security events. Threat analysis data can help security services detect attacks, understand them, and develop the most appropriate responses [7].

Denial of Service attack

A Denial of Service (DoS) attack overloads the target system with a large volume of traffic, impeding the system's ability to function normally. An attack involving multiple devices is known as a distributed denial of service (DDoS) attack [8].

The methods of Ddos attacks include:

HTTP flood DDoS- attacker uses HTTP requests that seem legitimate to overload the application or web server. This method does not require high bandwidth or distorted packets and usually tries to force the target system to allocate as many resources as possible for each request.

SYN flood DDoS - Initiating a connection sequence over the Transmission Control Protocol (TCP) involves sending a SYN request, to which the host must respond with a SYN-ACK, which confirms the request, and then the requesting party must respond with an ACK. Attackers can use this sequence by linking server resources by sending SYN requests, but not responding to the SYN-ACK from the host.

UDP flood DDoS - an avalanche of User datagram Protocol (UDP) packets sent to random ports is sent to the remote host. This method forces the host to search for applications on the affected ports and respond with "Destination Unreachable" packets that use host resources.

ICMP Flood - A stream of ICMP Echo Request packets overflows the target, consuming both incoming and outgoing bandwidth. Servers may try to respond to each request with an ICMP echo response packet, but they do not keep up with the speed of requests, so the system slows down.

Strengthening Network Time Protocol (NTP) NTP servers are accessible to everyone and can be used by an attacker to send large volumes of UDP traffic to the target server. This is considered an enhanced attack due to the ratio of requests and responses from 1:20 to 1:200, which allows an attacker to use open NTP servers to perform large-scale DDoS attacks with high throughput [9] .

Injection attacks

Injection attacks use various vulnerabilities to directly insert malicious data into the code of a web application. Successful attacks can reveal confidential information, perform a DoS attack, or compromise the entire system.

Here are some of the main vectors of injection attacks:

SQL Injection - An attacker enters an SQL query into an end-user input channel, such as a web form or a comment field. The vulnerable application will send the attacker's data to the database and execute any SQL commands entered in the query. Most web applications use databases based on Structured Query Language (SQL), which makes them vulnerable to SQL injection. A new variant of this attack is NoSQL attacks targeting databases that do not use a relational data structure.

Code injection - An attacker can inject code into an application if it is vulnerable. The web server executes malicious code as if it were part of an application.

OS Command Injection - An attacker can take advantage of a command injection vulnerability to enter commands to be executed by the operating system. This allows an attack to hijack OS data or hijack the system.

LDAP implementation - An attacker enters characters to modify LDAP requests. The system is vulnerable if it uses raw LDAP requests. These attacks are very serious because LDAP servers can store user accounts and credentials for the entire organization.

XML eXternal Entities (SXE) Injection - the attack is carried out using specially designed XML documents. This differs from other attack vectors because it exploits vulnerabilities inherent in outdated XML parsers, rather than unverified user input. XML documents can be used for path traversal, remote code execution, and server-side request forgery (SSRF).

Cross-site scripting (XSS) - an attacker enters a text string containing malicious JavaScript code. The target's browser executes the code, allowing an attacker to redirect users to a malicious website or steal session cookies to hijack the user's session. An application is vulnerable to XSS if it does not sanitize user input to remove JavaScript code [10].

REFERENCES

1. Internet Society is a global cause-driven organization governed by a diverseBoard of Trustees. http://www. internetsociety.org/sites/default/fi les/bp-deconstructingcybersecurity-16nov-update.doc.doc_RU_121712.pdf – article on the Internet «Views on cybersecurity: 2012.»
2.CNews – [electronic resource]. http://www.cnews.ru/ top/ 2013/ 03/13/ android_ zahvatil_kitay_vlasti_byut_ trevogu_522278 – article on the Internet «Android has conquered China. Authorities are sounding the alarm»
3. CNews|security [electronic resource] Sergey Popsulin – http://safe.cnews.ru/news/top/ index.shtml?2013/08/02/537614&utm_ source=twitterfeed&utm_medium=twitter – article on the Internet «the FBI is able to remotely activate the microphones in Android smartphones»
4. Securelist – [electronic resource] / Maria Garnaeva, Christian Funk /December 11, 2013/ http://www.securelist.com/ru/ analysis/208050822/Kaspersky_Security_Bulletin_2013_ Osnovnaya_statistika_za_2013_god. part of the report of Kaspersky Security Bulletin 2013 – «Kaspersky Security Bulletin 2013. Key statistics for the year 2013»
5. Vinokurov A.Yu. Traditional cryptographic algorithms. [Electronic resource] // Access mode: ww.enlight.ru/crypto/algorithms/algs. (date of access: 20.05.2021).
6. The Ministry of Internal Affairs assessed the damage from cybercrimes in Russia in 2019 [Electronic resource] // Official website of the KG television network - Access mode: https://russian.rt.com/russia/news/696185-mvdkiberprestuplenie-statistika (date of access: 01.07.2021).
7. The Prosecutor General's Office announced the low detection rate of cybercrimes [Electronic resource] // Official website of the Izvestia newspaper - Access mode: https://iz.ru/987854/2020-03-17/genprokuror-krasnov (date of access: 20.06.2021).
8. Cybercrime and cyber conflicts: Russia [Electronic resource] // - Russian Internet portal and analytical agency Tadviser on the topic of corporate informatization - Access mode: https://www.tadviser.ru/index.php/ (date accessed: 10.06. 2021).
9. Sidorenko E. On digital traces: only a quarter of cybercrimes are disclosed in the Russian Federation [Electronic resource] // Official website of the Izvestia newspaper - Access mode: https://iz.ru/962966/ elena-sidorenko / potcifrovym-sledam-v -rf (date accessed: 20.05.2021).
10. Center for Political Analysis and Information Security [Electronic resource] // Access mode: http://centerpolit.ru/content. php? id = 59 & now_month = 9 & now_year = 2014 (date accessed: 20.05.2021).