ANALYSIS OF DATA SECURITY PROGRAMS ON WEBSITES

Mahkamov Anvarjon Abdujabborovich
International Islamic Academy of Uzbekistan
"Modern information and communication
Technologies" department, associate professor, PhD
mahkamovanvar2020@gmail.com
Turdali Jumayev Saminjonovich
International Islamic Academy of Uzbekistan
"Modern information and communication
Technologies" department, associate professor, PhD
turdali240483@gmail.com

Annotation. This article provides an analysis of programs that ensure information security on web sites.

Ensuring the security of every web site created by this time is one of the most urgent problems today. Therefore, the statistics of how to ensure the security of the web sites that are being created today, through which program, are clearly presented in the tables.

Keywords: cyber security, cyber threat, web site, firewall, filter, information security, local network.

Introduction. Today, many businesses use PCs, networks, and servers to store their organization's critical data and manage their core operations. This emphasizes the importance of a good and reliable security system.

With the advent of advanced technologies, cybercriminals are also finding many ways to access the systems of many organizations and try to solve the problem in an easy and convenient way.

Organizations must not only protect their system from external factors, but also protect it from the inside. Some of the biggest cybersecurity threats are the result of errors and misuse by an organization's own employees and customers.

The 2018 Verizon Data Breach Investigations Report shows that 68 percent of data breaches take months or more to detect - a long time because the threats are not obvious.

Below, the extent of exposure to cyber threats of some sectors is given in percentage [3].

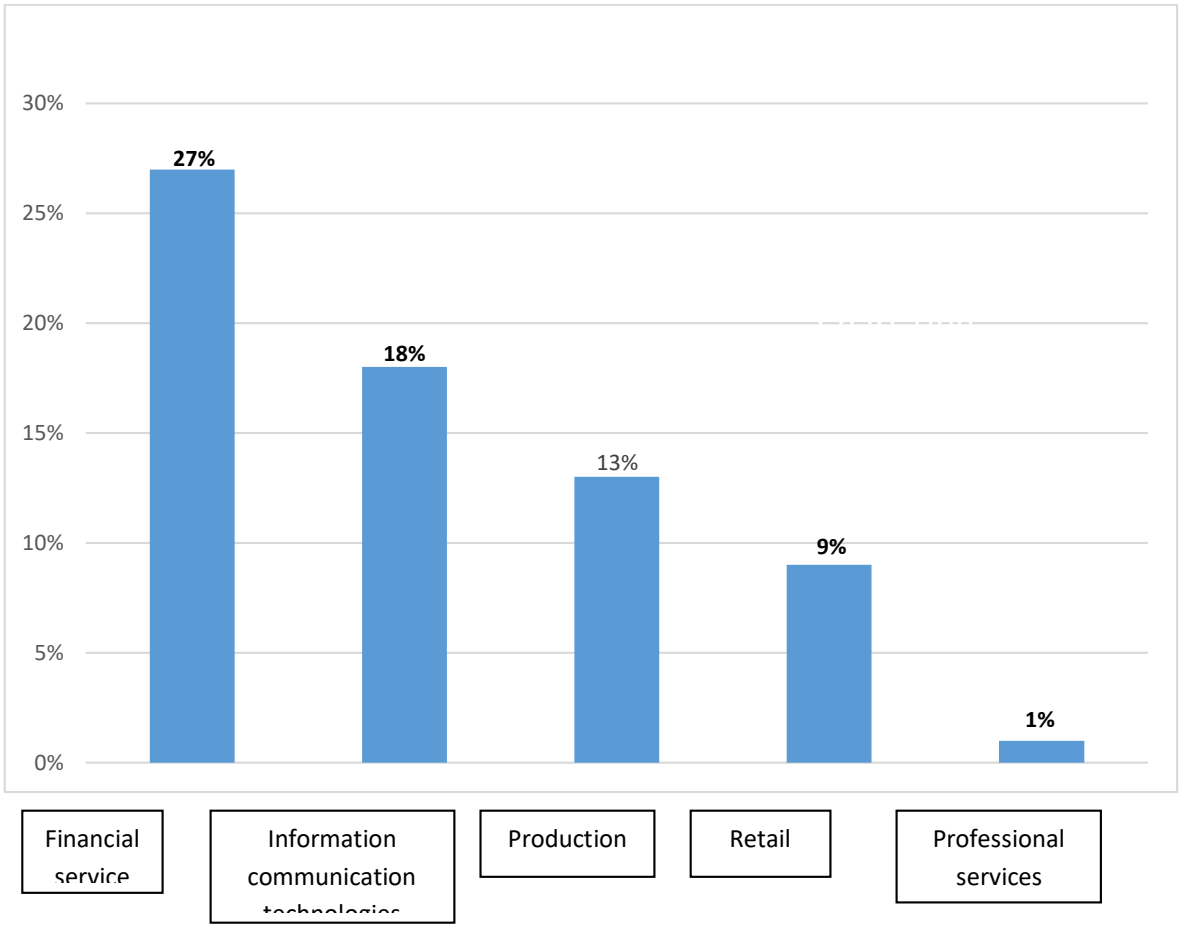

Figure 1. Volume of cyber threats by different sectors (percentage)

Based on the diagram above, it is worth noting that the financial services and information and communication technology sectors are the sectors most exposed to cyber threats. At the 2018 Cyber Security Business Insight Conference, panelists concluded that employees remain one of the biggest threats to system security.

Another study found that 24% of UK employees have admitted to intentionally disclosing and sharing confidential business information outside of their organization, such as new and former employees and even competitors.

The various types of anti-attack software mentioned above have been developed to detect and in some cases mitigate security attacks on various systems. Because there are different types of security attacks, there are different types of security products to target each of them.

Below are the most popular types of software and hardware that provide cyber security.

Firewall. A firewall is a software or hardware device that helps protect your network by filtering traffic and blocking unauthorized access to private information on your computer. A firewall can provide different levels of protection.

The firewall only accepts incoming connections that it is configured to accept. It does this by allowing or blocking certain data packets – the units of communication – that it sends over digital networks, based on pre-set security rules.

A firewall acts like a gatekeeper on a computer's access point or port, allowing only trusted sources or IP addresses. The principle of operation of the firewall is based on the control of traffic coming from outside. To manage traffic between LAN (Local area network) and external network, you can choose one of the following methods:

1. Batch filtering - based on configuring a set of filters. Depending on whether an incoming packet meets the conditions specified in the filters, it is forwarded or dropped on the network.

2. Proxy server - an additional proxy server device is installed between local and external networks, which acts as a “gateway” through which all incoming and outgoing traffic must pass.

3. Status Inspection - Inbound traffic inspection is one of the most advanced firewall techniques. Verification does not mean analyzing the entire packet, but only a part of its special key and comparing it with previously known values from the database of authorized resources. This method ensures the most efficient operation of the firewall [2].

In this way, the login can be configured only for the operation of any specific application, and potentially dangerous access can be prevented using all other protocols.

Spyware aniqlash dasturlari ham axborotni himoya qilish va tahdidlarni aniqlashda keng qo‘llaniladi va samarali usullardan biridir. Zararli va reklama dasturlari deb ham ataladigan josuslik dasturlari foydalanuvchi ixtiyorisiz kompyuterga o‘rnashib oladi va josuslik qiladi. Anti-Spyware dasturi esa kompyuter yoki tarmoqda ularning mavjudligini aniqlash va ularning o‘rnatilishini oldini olish yoki olib tashlash uchun ishlatiladi. Ularni o‘chirish juda muhim, chunki ular shaxsiy ma’lumotlarni kompyuterda “josuslik qilib” yozib oladi, shuningdek, hujjatlar, web sahifalarni ko‘rish va tugmalarni bosish kabi hisoblash xatti-harakatlarini yozib oladi. Bu esa kompyuterda reklamani moslashtirishi, uning konfiguratsiyasini o‘zgartirishi va hatto shaxsiy ma’lumotlarni boshqa masofaviy kompyuterga yuborishi mumkin.

Password protection. Password protection is an access control method that allows only valid credentials to log in. This allows you to protect important data from the actions of attackers. Password protection is one of the most common security tools. But attackers can easily bypass such protection if the characteristics of cyberattacks are not taken into account when creating combinations. To improve password protection, companies can implement a solution that blocks weak, easy-to-guess, and repetitive combinations.

Passwords are the first line of defense against unauthorized access to online accounts, devices, and files. Strong passwords help protect data from hackers and malware. The stronger the password, the better the data is protected. Using weak passwords is as dangerous as leaving your front door unlocked.

Hackers use different methods to steal passwords:

Removal attacks. All possible combinations for password cracking, account and system unauthorized access are simply sorted.

Change account information. Stolen usernames and passwords are automatically used to gain unauthorized access to online accounts.

Compare the combinatorics of all words in one Burmese dictionary.

Passwords are broken by entering dictionary words and their derivatives, replacing the letters in them with symbols, numbers or other letters.

Keylogging method. Special software controls all user manipulations using the keyboard. This allows you to obtain PIN codes, payment card numbers, usernames, passwords and other information.

Using malware. Special software damages computer systems, exploits their vulnerabilities, and is often used to steal passwords.

- password spray attacks. The same password is used for different login attempts. This will allow you to avoid blocking and stay out of sight.

Phishing. Attackers impersonate reputable organizations and service providers to trick users into providing them with credentials.

- Taking into account the above risks, various information security software have been developed.

Some of the key features of information security software are:

Automatic updates. This ensures that no updates are missed and is one of the most effective ways for information systems to respond to new cyber threats that are constantly emerging;

- real-time scanning. Dynamic scanning features make it easy to quickly identify and access malicious objects. Without this feature, it is much more difficult to prevent damage to your system;

- automatic cleaning. It is a feature that automatically gets rid of viruses when the user detects them, without having to manually remove them. This feature is effective in wasting time;

- multiple application protection. This feature ensures that all applications and services are protected, regardless of whether they are in email, messenger or web browser;

- application-level security. This allows application access control on a per-user role or per-user basis, ensuring that only trusted individuals access appropriate applications;

- role based menu. It displays menu options that display different users by role for easy access and management;

- multiple levels of security. This allows you to control access to data for a single application. This means that multiple users can be granted access to the same application, but control what information they are allowed to see;

- single sign-on. A session or user authentication process that allows users to access multiple related applications while being authorized in a single session by entering their name and password in only one place;

- user privilege settings. These are customizable features and security per individual user or role that can be accessed in their profile throughout each app;

- special information sources for the user. This allows you to create a single application that accesses different data sources depending on the user. This is the same as database-level security;

- application activity audit. It's critical for IT departments to quickly identify when a user is logged in and out, and which application they're logged into. Developers can log end-user activity using login/logout actions.

Conclusion. Information technology security software offers a number of advantages to the user. It’s worth noting that even the most professional users can download some form of malware or fall victim to online fraud and identity theft.

Preventing viruses, spyware, and identity theft is a serious matter. Professional hackers are finding sophisticated methods and algorithms to create viruses. Once these viruses settle on a computer, they can dramatically slow down processing speed, delete important data, and damage computer or network systems. Identity theft and spyware can be prevented by using software to protect sensitive personal information such as passwords, financial information, credit card numbers, and social security numbers of users of your system. In fact, 80% of cyberattacks are caused by weakly stolen passwords, so they need to be carefully protected.

USED LITERATURE

1. Fazilov, S. X., Mahkamov, A. A., & Jumayev, T. S. (2018). Algorithm for extraction of identification features in ear recognition. Информатика: проблемы, методология, технологии, 3-7.
2. Mahkamov, A. A., Jumayev, T. S., Tuhtanazarov, D. S., & Dadamuxamedov, A. I. (2024). Using AdaBoost to improve the performance of simple classifiers. In Artificial Intelligence, Blockchain, Computing and Security Volume 2 (pp. 755-760). CRC Press.

3. Zhumaev, T.S., Mirzaev, N.S., & Makhkamov, A.S. (2015). Algorithms for segmentation of color images based on the selection of strongly coupled elements. Studies of Technical Sciences,(4), 22(27),
4. Маҳкамов, А. А., & Инадуллаев, Х.Ў.Ў. (2021). Сравнительный анализ биометрических систем в обеспечении информационной безопасности. Universum: технические науки, (12-1 (93)), 32-37.
5. Махкамов А. А. Алгоритмы идентификации личности человека по изображению ушных раковин //Исследования технических наук. – 2015. – №. 4. – С. 28-32.
6. Tuhtanazarov, D., Xodjayeva, M., Jumayev, T., & Mahkamov, A. (2022, June). Computational algorithm and program for determining the indicators of wells based on processing of information of oil fields. In AIP Conference Proceedings (Vol. 2432, No. 1, p. 060021). AIP Publishing LLC.
7. Zhumaev, T. S., Mirzaev, N. S., & Makhkamov, A. S. (2015). Algorithms for segmentation of color images based on the selection of strongly coupled elements. Studies of Technical Sciences,(4), 22(27), 4.
8. Жумаев, Т. С., Мирзаев, Н. С., & Махкамов, А. С. (2015). Алгоритмы сегментации цветных изображений, основанные на выделение сильносвязанных элементов. Исследования технических наук, (4), 22-27.
9. Махкамов, А. А., & Дадамухамедов, А. И. (2022). Алгоритм выделения области ушных раковин при распознавании личности. Universum: технические науки, (5-1 (98)), 14-17.
10. Махкамов, А. А. (2015). Алгоритмы идентификации личности человека по изображению ушных раковин. Исследования технических наук, (4), 28-32.
11. Е.А.Степанов, И.К.Корнеев, Информационная безопасность и защита информации. – М.: Инфра, 2002.