UDC 004.94 **doi: 10.26906/SUNZ.2024.3.149**

D. Tyshchenko, T. Franchuk, R. Zakharov, V. Moskalenko

State University of Trade and Economics, Kiev, Ukraine

SUPPORTING DYNAMIC SECURITY NEEDS WITH VPN TOOLS

Abstract. The article examines the problems of supporting the dynamic security needs of a hybrid environment. It was determined that an important aspect of remote work is the training of employees on common cyber security threats. Threat types such as phishing attacks, social engineering, and malware are explored. The components of information technology security in a hybrid working environment are defined. The levels of protection of corporate information were studied. VPN features are analyzed. Security procedures for using VPN, which creates opportunities to reduce the risks of hacking a remote work environment, have been analyzed. Requirements to reduce the risks of unauthorized access to confidential information have been established. Disadvantages and limitations of VPN usage are explored. The criteria for reducing the connection speed due to additional cryptographic processing and the distance to the VPN server were analyzed. Methods and methods of blocking and limiting access to VPNs are considered, with the aim of reducing their effectiveness in some contexts. The features of a set of protocols that protect Internet Protocol (IP) communication by authenticating and encrypting all IP packets in the data stream are investigated. The principles of the VPN service are defined. Ways to prevent data misuse when working in a hybrid environment are proposed. Requirements for invulnerability of network traffic to attacks are defined. a set of protocols is explored, thanks to which it is possible to authenticate and check the integrity and encrypt IP packets. Analyzed protocols for secure key exchange on the Internet. The design of key information management protocols is proposed, requiring the development of the Internet Key Management Protocol. In the process of research, key management concepts were analyzed and improved using the ISAKMP specifications and the Oakley Key Determination Protocol. The criteria for the successful functioning of the ISAKMP specification, which describes the mechanisms for matching the attributes of the protocols used, have been established.

Keywords: hybrid working environment, cyber security, digital transformation, information security.

Introduction

The most important aspect is understanding cyber threats and the means to prevent them. The method of cyberattack prevention includes the use of VPN for a secure connection to the company's network, the installation of anti-virus software and information security monitoring systems.

The analysis of research results and the development of own means of ensuring the security of information technologies in a hybrid working environment aims not only to protect users from potential cyberattacks, but also to prepare them for the development of software products in the field of information security in the future.

Thus, cyber security management becomes a critically important aspect for basic scientific research and requires thorough analysis, particularly when working in today's digital environment.

The object of research is information technologies and their security in the context of hybrid work. The subject of the study is the analysis of the security of network connections, cloud services, virtual private networks (VPN), as well as the integration of various technological solutions used in remote work. In accordance with the stated object and subject of the research, the purpose of the work is to assess the existing security measures in the context of hybrid work, identify weak points and risks.

Analysis of recent research and publications. Examining the results of the work of modern researchers analyzing the presented issues, it should be noted that not all aspects of this topic have already been covered in scientific publications, which makes it possible to study this issue more thoroughly. Scientists take care of the challenges of supporting the dynamic security needs of a hybrid environment, studying such types of threats as phishing attacks, social engineering and malware. Based on the received data, we offer a methodology for protecting corporate information and security procedures for VPN use.

A number of sources testify to the analysis of the long-term strategy of IT security in the conditions of remote work In particular, O. Struuk analyzes a number of approaches and means of verifying the logic of the program developed by the user, in particular, he examines the logic of the program developed using the platform customization tool [1].

I. Arshad proposes a new framework for intelligent cyber defense, namely, studying immersion in deep learning attacks and defenses [2].

V. Pevnev considers methods and means of ensuring data integrity in information communication systems [3].

M. Ahola analyzes objective and subjective factors and errors in cyber security violations [4].

M. Rose describes the peculiarities of phishing, noting the best methods and methods of protection against it [5].

The study of the leading points and features of the implementation of VPN services on mobile devices deserves special attention, the results of research on their purpose, configuration, use, as well as the analysis of the best VPN services in Ukraine and the world are presented in numerous publications [6, 8, 15].

A. Kapiton, A. Mostova, V. Baranova, R. Baranenko, H. Sokol, M. Okhrymenko, T. Franchuk explore the communication possibilities of digital channels, pay attention to features of adaptive combined coding of the channel network for cognitive radio networks with cooperative relay [7, 11-14].

Main part

By studying the evolving telecommuting environment and understanding the reasons for its popularity, organizations can make an informed decision about implementing a telecommuting policy. Despite the undeniable benefits, remote work also creates unique cybersecurity challenges that organizations must address to protect sensitive data and systems. Research of real examples of cyber security violations in hybrid working environments allows to analyze and improve the methods of their detection and neutralization.

In particular, the SolarWinds Supply Chain Attack, known since December 2020, came into the field of our research. Attacks block access to files or systems, demanding a ransom.

That is why methods of detecting and neutralizing attacks need to be improved. Detection of attacks can be difficult due to their cunning and distributed nature, but regular data backups, protection of systems against viruses, and improved cyber hygiene help prevent or recover from such attacks[1-3].

This will ensure the highest level of protection for corporate information, as VPN encrypts all data transmitted between devices, including on open networks, which significantly reduces the risk of unauthorized access to confidential information.

While exploring potential drawbacks and limitations.

In particular, some VPN providers may collect log files of data about some activity that violates user privacy, some countries or organizations may block or restrict access to VPNs, making them less effective in some contexts, free or low-cost VPN providers may use public servers, which may be less secure or have limited bandwidth.

Given the growing number of remote workers and the associated cyber security threats, using a VPN is becoming a necessary standard for any organization looking to keep their data private and secure. Along with the right security policies and procedures, using a VPN can significantly reduce the risks of a remote work environment being compromised. Passwords remain a weak point in cyber security.

By choosing a certain criterion, it is possible to classify groups in a certain way VPN.

Thus, according to the method of technical implementation, the following VPN groups are distinguished, which are presented on Fig. 1.

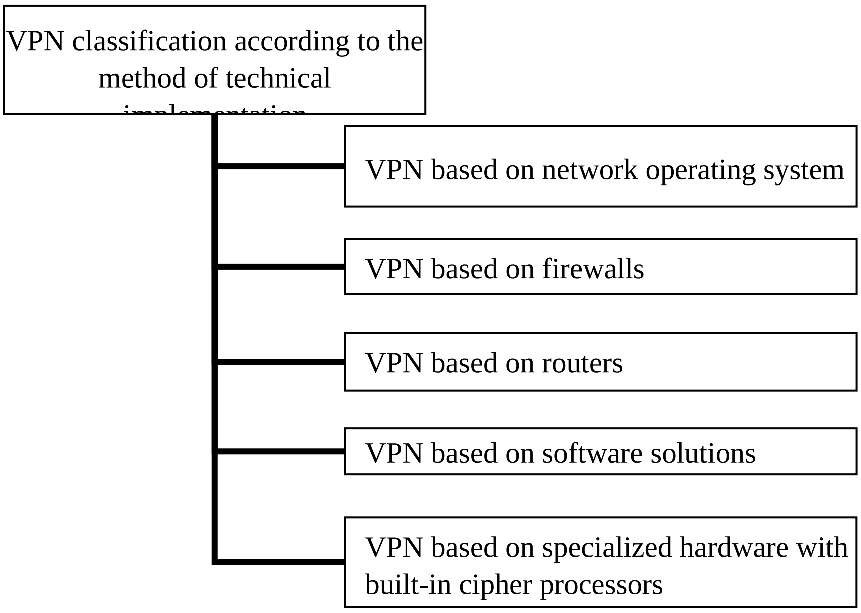
VPN classification according to the method of technical implementation
VPN based on network operating system
VPN based on firewalls
VPN based on routers
VPN based on software solutions
VPN based on specialized hardware with built-in cipher processors

Fig. 1. VPN classification according to the method of technical implementation

In addition, an important aspect is the remote management of security policies, which allows you to set and manage security rules on remote devices, for example, by restricting access or installing mandatory software updates. Additionally, mobile device security, such as disk encryption and remote data wipe capabilities, are important aspects of protecting remote endpoints.

Organizations should establish secure endpoint configurations that include active firewalls, use of up-to-date anti-virus software, and implementation of strong strong password policies. Educating remote employees about the importance of following these security measures on their devices is a key element of effective protection.

This helps create a consistent security system across all endpoints, providing a high level of protection against potential threats [6-8].

The user, in this case a QA engineer, is given an encryption key that must be connected to a PC for identification and access. This way of using VPN networks is used in almost all companies that have divisions in different geographical points or remote employees, including in a hybrid work environment. Analysis of access to blocked content deserves special attention. Sometimes the desired content is available only for a certain region or vice versa - it is allowed for all but one.

This problem is solved with the help of a VPN - the user's traffic is redirected through servers located in the country that has access to the necessary resources, while bypassing all regional blocks. The service in question is also used for testing applications from another country.

If the customer needs to test the operation of the application from different parts of the world, for example, due to the specifics of the application, then in order not to hire a large number of testers from different countries, it is enough to hire one team that will test using VPN networks.

In this case, you can connect to a remote server that will receive and transmit all device traffic.

Thus, the tester will receive the external IP address of this server and will be considered a user of this country.

Inter-corporate VPN networks provide company employees with a secure exchange of information with business partners, suppliers, wholesale customers, customers, users, etc.

An inter-corporate network provides direct access from one network company to the network of another, thus contributing to the increase in the reliability of the communication that is maintained in business cooperation.

In inter-corporate networks, much attention is paid to user authentication and access control using a network screen.

By understanding the tactics used by cybercriminals, employees can become more vigilant and proactive in protecting themselves and the organization's sensitive data. In addition, it is important to keep employees constantly trained and updated on the latest trends in cybersecurity, as these threats are constantly evolving. Organizations can also use phishing attack simulations to test their employees' reactions to real threats and improve their skills in detecting and preventing phishing. Training and supporting employees in the field of cyber security are important elements of an effective strategy to protect the organization from phishing attacks. This will allow to increase the awareness and preparedness of the personnel to detect and avert potential threats, which can solve the problem of phishing attacks to a significant level.

A VPN basically creates a secure data tunnel between your local computer and another VPN server located thousands of kilometers away. When using the Internet, this VPN server becomes the source of all data, so the ISP and other third parties can no longer see the content of your Internet traffic.

At the same time, the result of the negotiation of the security context is the establishment of the security parameter index (SPI), which is a pointer to a certain element of the internal structure of the information exchange party, which describes possible sets of security parameters. IPSec is a component of IPv6, operating at the third or network layer.

As a result, transmitted IP packets are protected in a manner that is transparent to network applications and infrastructure. Unlike SSL (Secure Socket Layer), which works on the fourth (transport) layer and is already associated with higher levels of the OSI model, IPSec is designed to provide low-level protection. An IPSec header is added to IP data ready for VPN transmission to identify protected packets.

Before transmission, these packets are encapsulated into other IP packets. IPSec supports several types of encryption, including Data Encryption Standard (DES) and Message Digest 5 (MD5). A necessary condition for establishing a secure connection is the ability to quickly agree on security parameters (authentication algorithms and keys).

IPSec supports two types of key management schemes by which participants can negotiate session parameters. This dual support at one time caused friction in the IETF Working Group.

Conclusions

Using traffic encryption, regularly updating software and network devices, and implementing monitoring and breach detection mechanisms will help prevent many types of cyberattacks.

In general, only a comprehensive approach to cyber security, which includes staff training, the use of secure technologies and the use of reliable protocols, can ensure the creation of a secure remote work environment that will effectively protect the organization's valuable assets.

Only this approach will ensure productive and safe work in a remote format.

A VPN is a good solution for establishing security and maintaining anonymity online, and it deserves the attention of anyone who uses the Internet on mobile devices or PCs. VPN networks provide a wide range of possibilities.

They are used not only by IT professionals, but also by ordinary users for various reasons.

In the process of using the possibility of limited authorization, in addition to the specified protection methods, additional special systems should be used to strengthen protection, taking into account the encryption tools used in the hybrid working environment of the corporation by means of VPN services.

Note that it is the logical network that is designed and created based on the use of the most widely used architecture model, which enables employees of the corporation and other users to work with the database during work.

When organizing work, in such a case, network administrators may implement additional special procedures to strengthen security.

Using the capabilities of the VPN service does not require additional work and does not pose a particular danger for testers.

It was determined that the design of key information management protocols is necessary, namely the development of IKMP, an application-level key management protocol.

The emerging key information management standards provide an opportunity to support Key Distribution Centers. Data integrity and confidentiality guarantees in the IPsec specification are provided through the use of authentication and encryption mechanisms, respectively, where the result of security context negotiation is the establishment of the SPI security parameter index.

REFERENCES

1. Striuk O. User-Designed Application Logic Verification Approach and Tools URL: https://radics.tech/user-designed-application-logic-verification-approach-and-tools/
2. Arshad I. A Novel Framework for Smart Cyber Defence: A Deep-Dive Into Deep Learning Attacks and Defences. *IEEE Access.* 2023. № 11. 88527-88548.
3. Pevnev V. Ensuring the Data Integrity in Infocommunication Systems *International Journal of Computing.* 2022. 228-233. URL: https://doi.org/10.47839/ijc.21.2.2591.
4. Ahola M. The role of human error in successful cyber security breaches. *Usecure Blog*. URL: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches.
5. Rouse M. What is email phishing? Definition, examples and best practices URL: https://searchsecurity.techtarget.com/definition/phishing
6. VPN on mobile devices: purposes, setup, usage URL: https://training.qatestlab.com/blog/technical-articles/vpn-mobile-device-setting/
7. Kapiton A., Kryvoruchko O., Tyshenko D., Franchuk T., Tsiutsiura M. Modern website creation technologies Комерціалізація інновацій в умовах Індустрії 4.0. Суми, СДУ, 2023. 145-153.
8. The best VPN URL: https://ua.cybernews.com/lp/best-vpn-ua/
9. Найкращі служби VPN в Україні URL: https://protonvpn.com/
10. Шифр-VPN URL: https://cipher.com.ua/uk/products/cipher-vpn
11. Mostova A., Kapiton A., Baranova V. Digital transformation of business in Ukraine: current trends, challenges and prospects. *Transformation of the economic system in the context of information technology challenges.* Riga, Latvia: Baltija Publishing, 2024. 70-86.
12. Kapiton A. Communication opportunities of digital channels. *Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану*. Хмельницький, НАДПСУ, 2024. 953-954.
13. Skakalina O., Kapiton A. Design and software implementation of a knowledge exchange web service. порівняльний аналіз застосування евристичних алгоритмів для розв'язання задачі TSP. *Системи управління, навігації та зв'язку*, 2024. 2 (76). 144-151.
14. Kapiton A, Baranenko R., Sokol H., Okhrymenko M., Franchuk T. Адаптивне комбіноване кодування мережі каналів для когнітивних радіомереж з кооперативною ретрансляцією. *Електронне моделювання*, 2024. 1. 78-89.
15. Bitdefender Premium VPN URL: https://www.bitdefender.ro/solutions/vpn.html

Received (Надійшла) 22.05.2024
Accepted for publication (Прийнята до друку) 14.08.2024

Підтримка динамічних потреб безпеки засобами VPN

Д. Тищенко, Т. Франчук, Р. Захаров, В. Москаленко

Анотація. У статті досліджено проблеми підтримки динамічних потреб безпеки гібридного середовища. Визначено, що важливим аспектом віддаленої роботи є навчання співробітників загальним загрозам кібербезпеки. Досліджено типи загроз, такі як фішингові атаки, соціальна інженерія та зловмисне програмне забезпечення. Визначено компоненти безпеки інформаційних технологій в гібридному робочому середовищі. Досліджено рівні захисту корпоративної інформації. Проаналізовано особливості VPN. Проаналізовано процедури безпеки використання VPN, що створює можливості зменшення ризиків зламу віддаленого робочого середовища. Встановлено вимоги до зниження ризиків несанкціонованого доступу до конфіденційної інформації. Вивчено недоліки та обмеження використання VPN. Проаналізовано критерії зменшення швидкості з'єднання через додаткову криптографічну обробку та відстань до сервера VPN. Розглянуто методи та способи блокування та обмеження доступу до VPN, з метою зменшення їх ефективності в деяких контекстах. Досліджено особливості набору протоколів, які захищають зв'язок Інтернет-протоколу (IP) шляхом автентифікації та шифрування всіх IP-пакетів у потоці даних. Визначено принципи роботи служби VPN. Запропоновано шляхи запобігання зловживанню даними, при роботі у гібридному середовищі. Визначено вимоги до невразливості мережевого трафіку до атак. досліджено набір протоколів, завдяки яким є можливість аутентифікувати та перевіряти цілісність та шифрувати IP-пакети. Проаналізовано протоколи для безпечного обміну ключами в Інтернеті. Запропоновано проектування протоколів керування ключовою інформацією, що вимагають розробки Internet Key Management Protocol. В процесі дослідження проаналізовано та вдосконалено концепції управління ключами з використанням специфікацій ISAKMP і протоколу Oakley Key Determination Protocol. Встановлено кретерії успішного функціонування специфікації ISAKMP, що описує механізми узгодження атрибутів використовуваних протоколів.

Ключові слова: гібридне робоче середовище, кібербезпека, цифрова трансформація, інформаційна безпека.