УДК 004.9 **doi: 10.26906/SUNZ.2024.3.126**

A. Kapiton[1], O. Dziuban[1], R. Baranenko[2], H. Sokol[3]

[1] National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine
[2] Uman National University of Horticulture, Uman, Ukraine
[3] National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

SECURITY OF INFORMATION TECHNOLOGIES IN A HYBRID WORKING ENVIRONMENT

Abstract. The article discusses the main aspects of information technology security in a hybrid working environment. With the rapid rise in popularity of remote work, traditional workplace security standards have been proven to be inadequate, creating a real need for effective cyber security measures. remote work has become the norm for many companies, but with it the threat of cyberattacks has also increased. Features and risks associated with the organization of a hybrid work environment caused by remote employment are considered, as well as methods of ensuring safety in such a work environment are investigated. The main problems that arise and need to be prevented have been identified. It has been proven that one of the key areas is to securely connect to corporate networks from remote locations. It has been established that traditional VPN methods can be ineffective or insufficiently secure in conditions of large-scale use, so it is necessary to use modern means of traffic encryption and authentication mechanisms, which aim to organize the protection of access to corporate resources. The article examines the content of the constituent components that are responsible for the security of the endpoint. Requirements are defined that allow access to update and modify the software and operating systems of remote devices, which is a special parts of the proposed strategy that meets data security for operation in a hybrid environment. The determining motives of the implementation of the main structural component mechanisms of data access control and the possibility of remote shutdown of devices in the event of emotional actions have been studied. data protection plays a crucial role in remote work. The indisputability of the need to design and implement a system for protecting all remote resources, means of recognizing and identifying suspicious messages and links, as well as the use of reliable passwords and two-factor authentication has been proven and substantiated.

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

Introduction

The current complex situation in the political and economic space has opened a new era of remote work, forcing organizations to rethink their cyber security strategies.

The result of the conducted research is the analysis and substantiation of ways to ensure the security of information technologies in a hybrid working environment and the study of methods of effective protection of a remote working environment. The goals of the study are to deepen the understanding of the conditions of remote work, to identify cyber security problems in this type of work, as well as to develop recommendations for ensuring the security of the remote work environment. The most important aspect is understanding cyber threats and the means to prevent them.

Attackers are constantly looking for vulnerabilities in systems and networks, especially in remote work environments. The study of methods of protection against phishing attacks, the use of unprotected Wi-Fi networks, as well as protection against the leakage of confidential information through remote access is an actual problem today.

As a result of constant modernization and rapid growth of work methods to overcome cyber threats, there is a need to improve information and communication, software and technical means. Note that today's security professionals focus on identifying and fixing software flaws, unlike users who have the ability not only to increase potential problems due to insufficient competence, but to prevent them.

Analysis of recent research and publications

Analysis of the works of leading scientists who expressed their opinions in materials published in magazines, collections of reports of conferences held in our country and abroad, gives confidence in the relevance of the researched issues. Buryachok V.L., Kyrychok R.V., the importance of information security in the conditions of remote work is investigated, various aspects of remote work are considered, in particular, security challenges and risks.

The researcher provides analytical information on the protection of remote connections, data protection and support of information security in a remote some working environment [1]. In the study of Buryachok V. L., Kyrychok R. V., the authors emphasize the concept of information security as a service in the context of remote work.

The authors emphasize the importance of service level agreements, continuous monitoring and incident response in a remote work environment [2]. Kavun S. V., Nosov V. V., Manzhai O. V. gives an idea of the technical aspects of remote access and control systems. Understanding these systems is essential to implementing effective security measures in a remote work environment [3].

Vazhnytskyi B. and Tkachev V. investigate the security aspects of multi-cloud environments and, after analyzing the causes of these problems, form their own criteria for a secure cloud based on them.

In their works, the main problems and reliability criteria of multi-cloud environments are outlined for their further analysis [4].

Al-Ammouri A., M. Dekhtyar, R. Ishchenko, E. Klochan, Lebid I., Dekhtiar M., Lyaskovskii V., Popova L., Tymchenko O., Poleva N., Podlevskyi B., Rykalyuk. P., Zhurakovskiy Yu., Poltorak V. Tulyakova N., Kulyk A., Kryvogubchenko S. research methods and means of information protection [5–10]. Serdyukov D., Severinov O., Sydorenko Z. consider the capabilities and deployment process of the ESET Mobile Device Connector (MDC) application in order to ensure the security and management of mobile devices in corporate environments [11].

Main part

Modern political and economic influences on the organization of employees' activities had consequences in the field of labor and contributed to the introduction of new methods in business. The rapidly growing demand for remote work forces organizations to fully or partially transfer employees to remote work with a remote access connection. Information security is of great importance for ensuring the vital interests of any state. The creation of a developed and protected environment is an indispensable condition for the development of society and the state, which must be based on the latest automated technical means. In general, the object of protection in the information system is information with limited access, which circulates and is stored in the form of data, commands, messages that have a certain limitation and value both for its owner and for a potential violator of technical information protection.

A violator is a user who has unauthorized access to information. The threat of unauthorized access is an event that qualifies as the fact of an attempt by the offender to commit unauthorized actions in relation to any part of the information in the information system. Let's consider possible channels of information leakage and options for unauthorized access to it: in the absence of a legitimate user, control and delimitation of access to the terminal, a skilled offender easily uses its functionality for unauthorized access to protected information by entering appropriate requests or commands; if there is free access to the premises, it is possible to visually observe information on the means of reflection and documentation, steal paper media, remove an extra copy, as well as steal other media with information: listings, magnetic media, etc.

A special threat is the uncontrolled downloading of software in which settings, properties, data, algorithms may be changed, a "Trojan" program may be introduced, or a computer virus may be rooted that performs destructive unauthorized actions. For example, recording information on a third-party medium, illegal transfer to communication channels, unauthorized printing of documents, violation of their integrity, unauthorized copying of important information, the importance of which is determined and limited to a very short or, on the contrary, a long time.

A dangerous situation is when the violator is an authorized user of the information system who, in connection with his functional duties, has access to one part of the information, and uses another part outside of his authority. There are many ways for an authorized user to break into an information system and obtain, modify, distribute, or destroy protected information. For this, you can use, first of all, privileged input-output commands, uncontrollability of authorization or legality of requests and requests to databases and data banks, servers, etc. During maintenance of the equipment, remnants of information on its media (hard disk surfaces, magnetic tapes and other media) may be detected. Erasing information using conventional methods (operating system tools, special software utilities) is ineffective from the point of view of technical information protection. The violator can renew and read its remains, which is why only special means of erasing the information to be protected are needed.

One of the important parts of comprehensive protection is access at the level of the operating system. Therefore, I consider it necessary to create user accounts and pass identification, authentication and authorization of users working in this operating system. Since the enterprise does not use a system of accounts and identification and authentication, I consider it necessary to implement it for more reliable data protection. To solve this problem, it is recommended to use the access matrix for granting rights and authorities for working with official information. Access delimitation is a set of procedures that implement the verification of access requests and assessment of the possibility of providing access based on the Access Delimitation Rules. Access restriction rules are a part of the security policy that regulates the access rules of users and processes to passive objects. When considering the interaction of two objects of a computer system acting as receivers or sources of information, one should distinguish between a passive object, which is operated on, and an active object, which performs or initiates this operation.

Analyzing data from a series of surveys by researchers, the group (APWG) concluded that the volume of phishing websites has increased by 47% between 2020 and 2023 (Fig. 1). A certain number of specialists, based on their duties, due to the possibility of working in a hybrid format, in most cases the targets of these attacks. It should definitely be noted about the advantages of hybrid work, especially remote, it creates difficulties in monitoring employee behavior. A report by A Tessian report found that forty-eight percent of employees state the fact more comfortable accepting security risks when working remotely [2, 12-14]. The growth of phishing attacks for 2021–2023 is presented in Fig. 1.

Using unsecured Wi-Fi networks carries significant risk, potentially exposing sensitive information to cybercriminals. In addition, the lack of physical security controls and increased reliance on personal devices create exploitable vulnerabilities.

The analysis of threats caused by cyberattacks in recent years allowed us to conclude that the largest number of cases related to the work of specialists at home, using a home network.

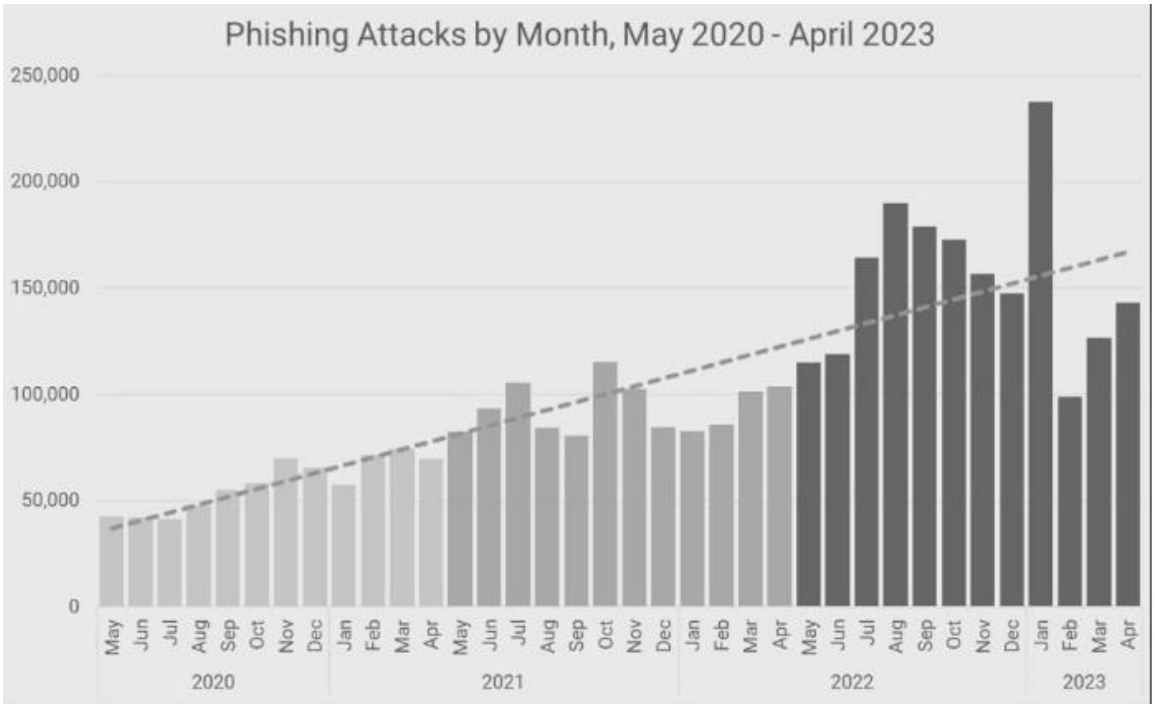

Fig. 1 Growth of phishing attacks for 2021-2023

That is why it can be argued that the security of the results of specialists' work in the conditions of hybrid work is insufficient, and measures to improve the cyber security strategy need to be strengthened. It is especially important to solve the task of implementing all possible protection methods, including the architecture of zero trust.

The minimum requirement of this concept is that users need to confirm the entered data at the time of performing a sequence of certain actions in the process of accessing resources [3-6].

Achieving work-life balance is essential to any flexible working environment. If there is a hybrid approach, it can enable employees to perform better. Additionally, home workers can schedule their days to take time off for important tasks, allowing them to be more flexible in their schedules and able to live and work wherever they want. Blended working helps people to better master their daily tasks when they need to take care of family (life or children), avoid long commutes, etc., which can increase concentration at work [12-15]. Ukrainian and global business leaders hold oppositely different opinions about what the working environment should look like in the next three years. 65% of global executives expect the office to become their primary work environment in three years. In contrast, Ukrainian company leaders continue to envision work in a hybrid format (88%), which is three times higher than the expectations of world leaders (28%).

Only 5% of Ukrainian managers talk about traditional office work. At the same time, managers both in Ukraine (5%) and in the world (7%) do not plan to transform the working environment into a format of completely remote cooperation.

The best hybrid collaboration tools for remote work presented in Table 1 [12-15].

Table 1 – **The best hybrid collaboration tools for remote work**

Confluence	Wrike	Trello
HighQ	InstaVC	GoVisually
Surfly	Asana	FlipBuilder
Adobe Workfront	Monday.com	FlipHTML5
Smartsheet	AnswerHub	Basecamp
Ziflow	Kissflow	Lucidspark

The application of data classification in remote work environments helps to increase the level of security and reduce the risk of privacy violations. Remote workers who clearly understand the importance of data protection and classification obligations can be more responsible in their work and compliance with security standards.

Thus, effective data classification is a key element of a cybersecurity strategy for remote work environments, enabling organizations to ensure reliable information protection and store sensitive data in a secure environment.

Conclusions

A hybrid model allows employees to participate in meetings virtually when needed and return to the in-person format for certain tasks or activities that require in-person interaction.

In addition, this approach provides employers with the necessary flexibility to plan for the future and make adjustments in changing conditions. Hybrid offices are increasingly becoming the new normal for many organizations around the world as they seek to offer

more balanced approaches to their employees in an ever-changing economic landscape. It's substantiated that ensuring IT security in remote work requires a comprehensive approach and design of advanced technologies and practices.

It is proposed to use the ISAKMP specification, which describes the mechanisms for agreeing the attributes of the used protocols and ensures a quick response to changing threats and constant updating of protection strategies, which are key to successful cyber security management.

By taking into account some precautions in advance, the company will be able to find solutions that will allow to use the possibilities of the new hybrid office as efficiently as possible. It goes without saying that creating a hybrid office can be extremely beneficial for both employers and employees. It becomes possible to use all the conveniences of the office and at the same time work in a comfortable environment that meets the needs of security.

Due to the fact that the security of remote work also depends on the awareness of users, it has been proven that training staff on cyber security issues, explaining potential threats and periodically monitoring the entire cyber protection system significantly reduces the risk of incidents.

REFERENCES

1. Бурячок В., Киричок Р. *Основи інформаційної та кібернетичної безпеки*. Київ: КУБГ, 2019. 320 с.
2. Гребенюк А., Рибальченко Л. Управління інформаційною безпекою. Дніпро: ДДУВС, 2020. 144 с.
3. Кавун С., Носов В., Манжай О. Інформаційна безпека. посіб. Харків: ХНЕУ, 2013. 352 с.
4. Vazhynskyi B., Tkachov V. Проблематика безпеки та критерії хнадійності мультихмарних середовищ. *Системи управління, навігації та зв'язку*. Полтава: ПНТУ, 2023, Т. 3 (73). 75-78.
5. Al-Ammouri A., M. Dekhtyar, R. Ishchenko, E. Klochan Методи та засоби захисту інформації. *Системи управління, навігації та зв'язку*. Полтава. ПНТУ, 2024. Т. 1 (75). С. 38-44.
6. Al-Ammouri A., Lebid I., Dekhtiar M., Lebid I., Al-Ammori H. Development of a mathematical model of reliable structures of information-control systems *Eastern-European Journal of Enterprise Technologies,* 2022. Vol. 5/9, Issue (119). С. 68–78.
7. Аль-Амморі. А., Лясковський В., Попова Л., Тимченко О., Полєва Н. Інформаційні системи та мережі. К-НТУ. 2021, 194 р.
8. Подлевський Б., Рикалюк. Р. Теорія інформації. Львів. ЛНУ, 2016. 342 р.
9. Жураковський Ю., Полторак В. Теорія інформації та кодування. К. Вища школа, 2011. 255 р.
10. Тулякова Н.. Теорія інформації. Суми. СумДУ, 2008.212.
11. Serdiukov D., Sievierinov O., Sydorenko Z. Особливості розгортання застосунку ESET mdm/mdc для забезпечення безпеки мобільних пристроїв. *Системи управління, навігації та зв'язку.* Полтава: ПНТУ, 2023, Т. 4 (74). С. 102-105.
12. The ultimate guide to building a hybrid desktop from scratch URL: https://fliphtml5.com/learning-center/uk/the-ultimate-guide-to-building-a-hybrid-workplace-from-scratch/
13. How hybrid work has affected the work of companies – research URL: https://news.finance.ua/ua/yak-hibrydna-robota-vplynula-na-robotu-kompaniy-doslidzhennya
14. 20 Best Hybrid Collaboration Tools for Remote Work URL: https://fliphtml5.com/learning-center/uk/top-20-hybrid-collaboration-tools/
15. CEE Cybersecurity Forum URL: https://dou.ua/calendar/46498/

Received (Надійшла) 03.07.2024
Accepted for publication (Прийнята до друку) 21.08.2024

Безпека інформаційних технологій
в гібридному робочому середовищі

А. Капітон, О. Дзюбан, Р. Бараненко, Г. Сокол

Анотація. У статті розглянуто основні аспекти безпеки інформаційних технологій в гібридному робочому середовищі. Доведено, що зі стрімким наростанням популярності віддаленої роботи традиційні стандарти безпеки на робочому місці є недостатніми, що породило реальну потребу в ефективних заходах кібербезпеки. Віддалена робота стала нормою для багатьох компаній, але разом з цим зросла й загроза кібератак. Розглянуто особливості та ризики, пов'язані із організацією гібридного робочого середовища, спричиненого віддаленим працевлаштуванням, а також досліджено методи забезпечення безпеки в такому робочому середовищі. Виявлено головні проблеми, що виникають та потребують їх попередження. Доведено, що однією з ключових областей є безпечне підключення до корпоративних мереж з віддалених місць. Встановлено, що традиційні методи VPN можуть бути неефективними або недостатньо безпечними в умовах масштабного використання, тому необхідно використовувати сучасні засоби шифрування трафіку та механізми автентифікації, які мають на меті організацію захисту доступу до корпоративних ресурсів. В роботі виконано аналіз ключових складових, що відповідають за безпеку кінцевих точок. Визначено вимоги, що уможливлює забезпечення актуальних патчів та оновлень для програмного забезпечення та операційних систем віддалених пристроїв, які є невід'ємною частиною стратегії забезпечення безпеки. Досліджена провідна роль розробки та впровадження механізму контролю за доступом до даних та можливістю віддаленого відключення пристроїв у разі виявлення підозрілих дій. захист даних відіграє критичну роль у віддаленій роботі. Визначена необхідність проектування та розробка системи захисту всіх віддалених ресурсів, засоби розпізнавання та визначення у підозрілі повідомлення та посилання, а також використання сильних паролів та двофакторної автентифікації.

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