УДК

Kudran S.P.
Boiko Y.V.

CYBER SECURITY ON THE INTERNET

Vinnytsia National Technical University

Анотація

Метою статті є визначення місця, ролі та функції кібернетичної безпеки. Кібербезпека відіграє важливу роль у секторі інформаційних технологій. Безпека інформації стала одним із серйозних викликів останнім часом. Щоразу, коли ми думаємо про інформацію та технології, що підвищують кібербезпеку, вперше, що спадає нам на думку, це кіберзлочини. Комп'ютерна безпека - це технологічний процес. У цій статті опубліковано дослідження мети кібербезпеки.

Ключові слова: кібербезпека, кібератака, кіберзлочинець, кіберзлочини, фішинг, мережа, пароль.

Abstract

The purpose of the article is to define the place, role and function of cyber security. Cybersecurity plays an important role in the information technology sector. Information security has become one of the serious challenges recently. Whenever we think of information and technologies that enhance cyber security, the first thing that comes to mind is cybercrime. Computer security is a technological process. This article explores the purpose of cyber security.

Keywords: cyber security, cyber attack, cyber criminal, cyber crimes, phishing, network, password.

Introduction

At the current stage of the latest information technologies cyber security, which contains an interagency character in a globalized world, is becoming more relevant. After all, cyber security is a human rights manifestation of the modern virtual world against the background of the innovative development of information technologies in the legal capital system. Cybersecurity is a set of processes, best practices, and technology solutions that help protect critical systems and data from unauthorized access. The main goal of cyber security is to protect people from cybercriminals on the information front [1].

Research results

The research paper then goes on to discuss the main functions of network security and the main purpose of cyber security. Cyber security goals to protect the users' confidential information from unauthorized access, and unidentified theft. It protects privacy and data and hardware that handles the store and transmits that data. Confidentiality is perhaps the category of the triad that most immediately comes to mind when a person thinks of information security. Data is confidential when only those people who are authorized to access it can do something to ensure confidentiality, a person needs to be able to identify who is trying to access data and block attempts by those without authorization. Password cracking, encryption, authentication, and defense against penetration attacks are all techniques designed to ensure confidentiality [2].

That means by which this principle is applied to an organization takes the form of a security policy. This isn’t a piece of security software and hardware rather than it’s a document that can be drawn up by an enterprise based on its own specific needs and quirks, to establish what data needs to be protected and secure and that’s the way.

These can be policies that guide the organizations in order to procure cyber security tools and also mandate the work behaviors and responsibilities.

There are also types of cyberattacks that you need to know about in order to be able to protect yourself from them [3].

Types of Cyber Security Attacks:

1. Email phishing attack
2. Drive by attack
3. Password attack

The first type of attack is phishing, which is a type of Internet fraud that involves the theft of confidential user data. Simply put, attackers trick users into revealing your personal information, such as phone numbers, bank card numbers and PINs, email and social media account logins and passwords [4]. To do this, we offer users some service or opportunity that attracts them to such actions.

The second type is drive by attack downloads attacker files are a common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTPs and PHP code of the pages. This script might be installed malware directly into the drive of someone who visits that site or it might redirect the sufferer to a site controlled by the attacker. To protect the sufferer from being driven by an attacker, the victim needs to keep your browser and operating system up to date and avoid websites that might contain malicious code. Hacker distributed malware by poisoning legitimate websites. Hacker injects malicious frames into HTML content.

The third type is password attack [5]. Often, an attacker wants to guess a user's password by typing it. In this case, you should set passwords using a set of letters and numbers, without tying it to the names of close people or to your own name. also don't set a password that consists of someone's birthday because that's too cheesy. If the software product is well protected, the user will receive a message that someone intends to visit his page.

Conclusion

That day was general security facing issues and already an international problem that all countries are trying best level of address at international level. The increasing of daily life use of internet and issuing cyber security problems and how to face these problems popularity of the internet as a medium and its borderless, interconnected to nature seeks and exacerbate the security situations and which not be assumed and taken for granted because many countries have been very bad experiences related to most of the hard or critical problems and so many problem facing to financial and painful memories.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cybernetic Security and Business Intelligence in the System of Diagnostics of Economic Security of the Enterprise [Електронний ресурс]. Режим доступу: https://pathofscience.org.
2. Войцих Н.М. Державна політика в українському інформаційному просторі: стан та проблеми [Електронний ресурс] / Н. Войцих // Режим доступу : http://www.ijimv. knukim.edu.ua/zbirnyk/1_2/2-vojzih.pdf.
3. What is information security? Definition, principles, and jobs [Електронний ресурс]. Режим доступу: https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html
4. Що таке фішинг і фішингова атака? [Електронний ресурс]. Режим доступу: https://hostiq.ua/blog/ukr/internet-phishing.
5. How to Create a Secure Password? [Електронний ресурс]. Режим доступу: https://www.wikihow.com/Create-a-Secure-Password.

Автор: Кудрань Софія Павлівна – студентка групи 5ПІ-22б, факультет інформаційних технологій та комп’ютерної
інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: sofia.kudran@gmail.com.

Співавтор: Бойко Юлія Василівна, старший викладач кафедри іноземних мов, ВНТУ, e-mail : boiko@vntu.edu.ua.

Author: Kudran Sofia – student of the 5PI-22b group, faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: sofia.kudran@gmail.com.

Co-author: Boiko Yuliia, senior teacher of foreign languages department ,VNTU, e-mail : boiko@vntu.edu.ua.