**Paper Title (Times, 14, Bold)**

Author (Times,12)

*E-Mail, OrcID,
University/Institution, Department, City, Country*

***ABSTRACT: (Times, 10, Bold)*** *Today, with the introduction of information technologies and the Internet into many sectors, it has been seen that great risks have emerged in the field of software. There are a lot of users who use it without knowledge of cybersecurity, especially on social media. These users bring a major security vulnerability to the cyber environment they are in. In particular, security gaps in infrastructure-related sectors such as the energy sector can cause enormous damage. Information security refers to measures based on the elimination of weaknesses caused by information technologies. The software that makes up these technologies is developed with programming languages. Many of the developers are unaware of the vulnerabilities and precautions. TCP/IP, the communication protocol used by the Internet, was developed in 1983. A lot has changed since then. Vulnerabilities in this protocol have been continuously patched. If we are using a protocol that is not very solid, we need to have basic security concepts.*

*In this study, the dangers to software security for developers and users will be identified. The necessity of having basic knowledge of software security will be emphasized. Techniques for combating attacks that can penetrate security will be revealed.*

***KEYWORDS: (Times, 10, Bold)*** *Software Security, Internet Communication Protocol, Sql*

Date of Submission: dd.mm.yyyy Date of Acceptance: dd.mm.yyyy

1. **INTRODUCTION (Times, 11 Bold)**

The world of informatics is developing quite rapidly and is taking us all under its control in a very wide area. The data community, known as Big Data, is growing day by day. This data is our information. The size of the danger increases significantly as the data falls into the hands of malicious people or institutions. With all the control in the information world under the control of one or several institutions, the wars for supremacy are getting hotter.

These wars also affect strategies between countries. Thanks to the fact that data is kept on their servers under the name of cloud technology, the project or important information of many people in the world has come into their hands like a hair from butter. It is also noteworthy that artificial intelligence-supported software that can pull out meaningful ones or useful ones from the information in Big Data is run day and night. For cloud technology pioneers, we can count Google Drive and Microsoft OneDrive examples.

1. **METHODOLOGY**

In this study, the security of data exchange with software that provides control of information will be emphasized. It will be tried to explain what the necessary measures are. It will be explained which measures will be used to increase the level of software security. Very important steps to be known during the process of transferring the information to the digital environment in an irrepressible way will be explained.



***Figure 1 (If table, title will be “Table”): The software development cycle***

1. **DISCUSSION**

Software development is a long-term process based on a wide infrastructure. It is very important to work systematically in this process. In general, in software developed with one or several people, security stages are not used much. As a result, software with low security vulnerabilities will emerge. In software companies that are more corporate, systematic work has an important place. Secure software affects our future. Every software is like a growing seed. As it grows, it gives benefits to its surroundings. It matures according to the situation. Software developers must be trained on threats. They must be ensured to have basic safety knowledge.

1. **FINDINGS**

All living things have their own life cycle. For example, human; they are born, grow, age, die, mix with the soil and become the source of other lives. Similarly, there is a cycle in every area of life. As computer engineers, when we are going to do a project, we set a cycle and develop and present the software within this cycle. Therefore, we should know that software has a life cycle of its own. Software Development Life Cycle in general; is the set of steps determined to be implemented during the development and maintenance of a software. What should not be forgotten is that since the functions and needs of software are constantly developing and changing, there is no one-way right part of the software, it is a cycle that repeats and renews itself.

1. **CONCLUSION (11 Bold)**

In this article, we've covered the major threats and defense strategies in cybersecurity. Our research and analysis have shown that cybercrime is increasing day by day and the attackers are constantly changing their methods with the developing technologies. At the same time, it has been understood that cyber attacks, which have serious consequences for companies and individuals, cannot be prevented with traditional security measures.

Our key results are:

Human Factor: It has been seen that the human factor is important in terms of cyber security. Education and awareness programs are an effective method in making users more aware and prepared against cyber threats.

Advanced Threats: With the developing technologies, advanced threats are increasing. Taking a proactive approach to these threats is important in preventing cyber attacks.

Security Solutions: Layered security solutions are one of the most effective defense methods against cyber attacks. Measures such as firewalls, security software, and constant monitoring help detect and block threats.

Our recommendations:

Training and Awareness: Institutions and individuals should raise awareness of employees and users on cyber security through regular training. This will help in reducing the success of social engineering attacks.

Advanced Threat Monitoring: Companies should set up advanced threat monitoring systems and take a proactive stance against cyber attacks. Particular attention should be paid to the detection and prevention of advanced threats such as data theft and spyware.

Collaboration and Sharing: Companies should increase cross-industry collaboration and effectively share threat information about cyber attacks. In this way, it will be possible to detect and prevent threats more quickly.

As a result, cybersecurity is an increasingly complex topic and needs to be constantly updated. By addressing prominent threats and defense strategies in this article, we aimed to provide readers with essential information to increase their security. However, being vigilant about security and constantly following developments are important for a successful fight against cyber threats.

**REFERENCES**

ALTINKAYNAK M., (2017). Applied Cyber Security and Hacking, Abacus Publications, İstanbul

DEMİR B., (2013). Software Security Attack and Defense, Dikeyeksen Publications, İstanbul

OF M., (2018). Basic Tips of Information Security Policies, Enscon 18 Spring Symposium, http://enscon.org/pdf/ensontammetinbildirikitabi.pdf

OpenSAMM, http://www.cs.unh.edu/~it666/reading\_list/SDLC/opensamm\_1.0.pdf, (Access Date: 05.06.2021)

Information Security Specialist Employment, https://www.f5haber.com/emlak-eki/havelsan-turkiye-de-15-bin-siber-guvenlik-uzmani-haberi-5795144/, (Access Date: 05.05.2021)