https://gospodarkainnowacje.pl

GOSPODARKA I INNOWACJE

LABORATORIUM WIEDZY Artur Borcuch

Volume: 45 | 2024

Economy and Innovation
ISSN: 2545-0573

For more information contact: editor@gospodarkainnowacje.pl

PREVENT AND RESPOND TO CYBER SECURITY THREATS

MukhammadAli Odilov Shukhratbek ugli
Lincoln University

ARTICLEINFO.

Keywords: cyber security, computer networks, cyber security threats, software, cyber attacks.

Abstract

Security is the state of being safe and free from danger or threat.So, if we put the two words together, "cyber security" refers to keeping computers, networks, and any device connected to the Internet safe from any danger or threat.This article provides information on data analytics to predict, prevent, and respond to cyber security threats.

Cyber security is the method of protecting computer networks and systems from digital attacks. These attacks can take the form of viruses, malware, phishing scams, and more. Cyber attacks can have serious consequences: financial losses, data corruption, and even physical damage. That's why it's so important to take steps to ensure cybersecurity for yourself, your family, and your business. One of the most common cybersecurity threats is malware. These are software designed to damage or disable computers. This virus can be caused by a Trojan horse, worms or spyware. Malware can be used to steal compromised data, delete important files, or control the victim's computer. Another common type of threat is a cyber attack. In this, a hacker attempts to gain unauthorized access to a computer system or network in order to steal data or disrupt operations. Cyberattacks can be very sophisticated and targeted or relatively simple and indiscriminate. System vulnerabilities, on the other hand, are a type of threat that cybercriminals can exploit. These are weaknesses in a computer system or network that can be used to gain unauthorized access or damage. Common vulnerabilities include unpatched software, weak passwords, and open ports.

Types of cyber security threats.

There are different types of attacks in cyber security and they can come from different sources. The most common viruses, malware, phishing scams and Denial of Service (DoS) attacks. Cyber security threats can have a variety of effects, from causing financial damage to compromising confidential information. Cyber security threats can in some cases allow attackers to gain control over critical infrastructure or devices, while in other cases they can threaten physical security.

The most popular cyber security threats are:

Malware is a cyber security threat that can take many forms, including viruses, worms, Trojan horses, and spyware. Malware can damage or disable a computer, steal information, or gain access to confidential information. In some cases, the malware can even be used to control the victim's computer.

Trojan virus: A type of malicious software that makes users think they are downloading a healthy file, even though the file is malicious. Once the file is executed, the Trojan virus gives the attacker access to the victim's system, allowing them to perform malicious actions such as stealing data or installing more malware.

Worm: A type of malware designed to spread itself by replicating itself and sending itself to other systems. Worms can cause a lot of damage because they can spread quickly and consume a lot of resources, which can crash systems.

Ransomware: This type of malware encrypts the victim's files and then demands a payment to decrypt the files. This can be a very costly attack for the victim as they may not be able to access their core files until they pay the ransom.

Spyware: Malicious software designed to secretly collect information about victims from them. This information can be used to track the victim or steal their identity.

Wiper Malware: Malicious software designed to delete files or cause a system crash. This type of malware is often used in aggressive attacks that aim to cause as much damage as possible.

Cyber threat intelligence (CTI) is knowledge, skills, and experience-based information about the occurrence and assessment of cyber and physical threats and threat actors to help mitigate potential attacks and malicious events in cyberspace.

Cyber threat intelligence sources include open source intelligence, social media intelligence, human intelligence, technical intelligence, device log files, forensic data or intelligence from internet traffic, and data for the deep and dark web. information is included.

In recent years, threat intelligence has become an important part of companies' cybersecurity strategies, as it allows companies to be more proactive in their approach and identify which threats pose the greatest risk to the business.

This puts companies on a more proactive front – actively trying to find their vulnerabilities and prevent hacks before they happen. the most common method is the use of threats (47% of all attacks).

Vulnerability to threats has increased in recent years due to the COVID-19 pandemic and more people working from home – making companies' data even more vulnerable. On the one hand, due to the increasing number of threats and the complexity required for threat intelligence, many companies in recent years have chosen to outsource their threat intelligence activities to a managed security provider (MSSP). Cyber threat intelligence (CTI) in brief - Hackers are working to find new ways to stay ahead of security software and breach organizations' networks, so it's important that security professionals use proactive best practices to prevent incidents.

Conclusion:

Hackers are working to stay ahead of security software and find new ways to breach organizations' networks, so it's important that security professionals use proactive best practices to prevent incidents. One of the best ways to do this is to understand and assess your organization's cyber threat intelligence and then apply that knowledge to ongoing efforts. With the right cyber threat intelligence, you can take every step towards the best cyber security possible.

References:

1. F. Mukhtorov, A. Umarov, A. Rozaliyev "CLASSIFICATION OF SECURITY THREATS IN INFORMATION SYSTEMS", "Engineering problems and innovations" scientific journal.
2. Dostonbek T., Jamshid M. Use of Artificial Intelligence Opportunities for Early Detection of Threats to Information Systems //Central Asian Journal of Theoretical and Applied Science. - 2023. - T. 4. - no. 4. - S. 93-98.
3. MIRZAYEV J. B., TOJIMATOV D. H. O. G. L. I. PUBLIC POLICY ON PROVIDING CYBER SECURITY AND PREVENTING CYBER ATTACKS -S. 36-37.

4. Mukhtorov F. M. et al. ANALYSIS OF INFORMATION SECURITY RISKS "Descendants of Al-Fargani" electronic scientific journal of Fergana branch of TATU named after Muhammad al-Khorazmi ISSN 2181-4252 Volume: 1 | Number: 3 in 2023
5. https://uzcert.uz/usefulinfo/prognoz-osnovnykh-riskov-kiberbezopasnosti-na-2021-god/