CYBER SECURITY

Shaxakimova Mavjuda Tashpolatovna
Docent of TUIT
Zokirova Shaxnoza Olimjon qizi
student of Alfraganus university

Annotation: *This article covers the topic of kiber security. The article provides information about the security threats faced by internet users and the precautions that can be taken against these threats.*

The beginning of the article emphasizes the importance of kiber security. With the widespread use of the Internet, the risk of personal data and sensitive information being stolen or misused has increased. Therefore, individuals and institutions need to be aware of cyber security.

The rest of the article discusses common cyber security threats. These include threats such as viruses, ransomware, phishing attacks and data leaks. Each threat is explained in detail and suggestions are offered on how to protect yourself.

In the last part of the article, kiber security measures are mentioned. Precautions such as using strong passwords, having up-to-date antivirus programs and choosing reliable websites are recommended for internet users. It is also emphasized that institutions should take precautions such as firewalls, network monitoring systems and personnel training.

This article provides general information about cyber security. It is intended that readers take their own security precautions and be aware of current threats.

Keywords.

Cybersecurity, individuals, systems, processes, Technology Evangelist, cyber attacks, Application Security, ransomware, IT security, Cloud security, Infrastructure Security, Network security, implementing, cyberattacks, information security, definition, complement, management system, Similarly, James Stanger, Security products,

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

Every square IS a rectangle because a square is a quadrilateral with all four angles being right angles. Similarly, cybersecurity IS a part of the IT security umbrella, along with its counterparts, physical security and information security.

But not every rectangle is a square, since the criteria to qualify as a square means all sides must be the same length. The point is, not all IT security measures qualify as cybersecurity, as cybersecurity has its own distinct assets to protect.

CompTIA's Chief Technology Evangelist, James Stanger says it best when he defines cybersecurity as "focusing on protecting electronic assets – including internet, WAN and LAN resources – used to store and transmit that information."

Of course, the threat to these electronic assets are hackers who have malicious intent to steal proprietary data and information via data breaches. Thus, it would seem the fully realized definition should include an evolving set of cybersecurity tools designed to protect confidential data from unauthorized access. To do so, it's necessary to consider how people, processes and technology all play equally important roles in keeping information safe.

Why Is Cybersecurity Important?

One of the many advantages to living in a world where every device is connected is convenience. It's incredibly easy to conduct work, manage your social calendar, shop and make appointments from your smartphone or device. That's why it's become second nature to many of us.

But, of course, the convenience of connected data also means threats from bad actors can do a lot of damage. Cybersecurity initiatives are essential to protecting our data and thus, our way of life.

A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber attacks. A unified threat management system can automate integrations across select Cisco Security products and accelerate key security operations functions: detection, investigation, and remediation.

A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber attacks. A unified threat management system can automate integrations across select Cisco Security products and accelerate key security operations functions: detection, investigation, and remediation.

Cybersecurity refers to any technology, measure or practice for preventing cyberattacks or mitigating their impact. Cybersecurity aims to protect individuals' and organizations' systems, applications, computing devices, sensitive data and financial assets against simple and annoying computer viruses, sophisticated and costly ransomware attacks, and everything in between.

The information technology (IT) trends of the past few years the rise in cloud computing adoption, network complexity, remote work and work from home, bring your own device (BYOD) programs, and connected devices and sensors in everything from doorbells to cars to assembly lines have resulted in tremendous business

advantages and human progress, but have also created exponentially more ways for cybercriminals to attack.

Despite an ever-increasing volume of cybersecurity incidents worldwide, and ever-increasing volumes of learnings gleaned from them, some very dangerous misconceptions persist.

Strong passwords alone are adequate protection. Strong passwords make a difference. For example, all other things being equal, a 12-character password takes 62 trillion times longer to crack than a 6-character password. But because cybercriminals can steal passwords (or pay disgruntled employees or other insiders to steal them), they can't be an organization's or individual's only security measure.

The major cybersecurity risks are well known. In fact, the risk surface is constantly expanding. Thousands of new vulnerabilities are reported in old and new applications and devices every year. And opportunities for human error specifically by negligent employees or contractors who unintentionally cause a data breach keep increasing.

All cyberattack vectors are contained. Cybercriminals are finding new attack vectors all the time including Linux systems, operational technology (OT), Internet of Things (IoT) devices, and cloud environments.

One of the most problematic elements of cybersecurity is the evolving nature of security risks. As new technologies emerge, and as technology is used in new or different ways, new attack avenues are developed. Keeping up with these frequent changes and advances in attacks, as well as updating practices to protect against them, can be challenging. Issues include ensuring all elements of cybersecurity are continually updated to protect against potential vulnerabilities. This can be especially difficult for smaller organizations without adequate staff or in-house resources.

Here are the some common types of cybersecurity available:

Application Security: Application security refers to the measures integrated into applications during their development to safeguard the data or code within them from theft or highjacking, according to VMWare, and these protective mechanisms are designed to shield the application post-development.

Cloud Security: Cloud security is the amalgamation of technologies and strategies designed to protect data, applications and the associated infrastructure of cloud computing environments from both internal and external threats, according to Skyhigh Security, aiming to prevent unauthorized access and ensure the overall security of data in the cloud.

Infrastructure Security: Critical infrastructure security describes the physical and cyber systems that are so vital to society that their incapacity would have a debilitating impact on our physical, economic or public health and safety, according to CISA.

Internet of Things (IoT) Security: IoT is the concept of connecting any device to the internet and other connected devices. The IoT is a network of connected things and people, all of which share data about the way they are used and their environments,

according to IBM. These devices include appliances, sensors, televisions, routers, printers and countless other home network devices. Securing these devices is important, and according to a study by Bloomberg, security is one of the biggest barriers to widespread IoT adoption.

Network Security: Network security is the protection of network infrastructure from unauthorized access, abuse or theft, according to CISCO, and these security systems involve creating a secure infrastructure for devices, applications and users to work together.

FOIDALANILADIGAN ADABIYOTLAR:

1. G’aniyev S. K. ,Karimov M. M., Tashev K. A. AXBOROT XAVFSIZLIGI Toshkent 07
2. S.S. Qosimov Axborot texnologiyalari xaqida o’quv qo’llanma Toshkent 07
3. G’aniyev S.K.Karimov M.M. Hisoblash tizimlari va tarmoqlarida axborot xavfsizligi TDTU 03 4. http://www.kaspersky.ru/
5. http://www.viruslist.ru/
6. http://www.citforum.ru/internet/infsecure/its2000_01.shtml/
7. http://www.osp.ru/lan/2001/04/024.htm/
8. http://www.osp.ru/lan/2001/03/024.htm/
9. www.nasa.gov/statistics/
10. www.security.uz/
11. www.cert.uz/
12. www.uzinfocom.uz/