ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

ACROPOLIS
Enlightening Wisdom

BTech: III Year

Department of Computer Science & Information Technology

Name of the Student : Kundan Goswami

Branch & section : CSIT -2

Roll No. : 0827CI201100

Year : 2022-23

Department of Computer Science & Information Technology

AITR, Indore,

Introduction

Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems. With an increasing number of users, devices and programs in the modern enterprise, combined with the increased deluge of data -- much of which is sensitive or confidential -- the importance of cybersecurity continues to grow. The growing volume and sophistication of cyber attackers and attack techniques compound the problem even further.

List of cyber security technologies :

1. Artificial Intelligence & Machine Learning
2. Internet of Things
3. Blockchain
4. Cloud computing
5. Web security
6. Application Security
7. Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
8. Data Loss Prevention (DLP) & Data encryption
9. Firewalls
10. Social engineering or insider threat

1. Artificial Intelligence & Machine Learning:

Artificial Intelligence: Artificial Intelligence is the simulation of human Intelligence into the machines that are programmed to think as humans do and imitate their actions. This term can also be used for any machine which exhibits characteristics related to the human mind, like learning and problemsolving. The ideal feature of AI is its ability to simplify and undertake actions that are most likely to achieve a particular goal. Artificial Intelligence allows machines to learn from experience, adapt to new inputs, and carry out tasks similar to those of man.

2. Internet of Things:

The Internet of Things is about connecting any device with the Internet or other connected devices. The IoT is a huge network of connected objects and people who gather and share data about how they are used and the environment around them. It includes a number of objects of various sizes and shapes, from smart microwaves to self-driving cars, to wearable fitness devices.

3. Blockchain:

Blockchain is a system for storing information in such a way that it is very difficult and impossible to hack, cheat or change the system. A blockchain is basically a digital ledger of transactions which is duplicated and distributed throughout the whole network of computer systems on the blockchain. Every block in the chain holds certain amounts of transactions, and whenever a new transaction occurs on the chain, a record of this transaction will be added to all the participant's ledgers. The decentralized database handled by a number of participants is referred to as Distributed Ledger Technology.

4.Cloud Computing:

Cloud Computing is the provision of a number of services over the Internet. This resource contains applications and tools such as databases, servers, data storage, software, and networking. Instead of retaining the files on a local storage device or proprietary hard disk, cloud-based storage allows them to be stored in a remote database till the electronic device has access to the Web; it can access information and software programs for executing it.

5. Web security:

Essentially, the Internet is an excellent way to connect to the whole world. We use the Internet as a means of connecting with others for sharing information, files for entertainment, socializing, and so on that might be helpful to us. Mobile technology, however, has enabled a much wider spread of the Internet, increasing the number of Internet users all over the world. The Internet remains the most democratic mass media. With very little investment, everyone can get a Web page on the Internet.

6. Application Security:

Applications are software's that allow the user to carry out specific tasks on a mobile device or computer. People look to apps to make life easier for them, and they are most likely to use them if it serves a particular purpose. Our research has shown that 2 out of 3 people will use an app frequently as it makes their lives easier. Mobile applications provide the ultimate convenience. You can order dinner, take a ride, and do many things from your phone. Some research suggests that revenues from global applications are projected to rise steadily from year to year.

7. Intrusion Detection System (IDS) and Intrusion Prevention System

IDS refers to the Intrusion Detection System. An IDS is intended to detect and monitor intrusions, and it requires human assistance or automated systems for interpreting the results and deciding whether to act or not.

IPS refers to the Intrusion Prevention System. An IPS may choose to accept or reject packages depending on the rules. It must be updated to recognize the most recent threats.

8. Data loss prevention (DLP) & Data encryption:

Data loss happens when precious or sensitive information on the computer is compromised as a result of theft, software corruption, viruses, malware, human error, or power failure. It can also be caused by mechanical failure, physical damage, or building equipment. It is frequent for the data to obtain "lost" data to get corrupted or deleted unintentionally. For example, dropping the laptop hard drive may easily result in data loss or corruption, like malicious software or computer virus.

9. Firewalls:

A network security device which monitors the incoming and outgoing network traffic and chooses if it can allow or block specific traffic according to the set of security rules defined. A firewall may include software, hardware, or both. Firewalls are very important as they have had an enormous influence on modern security techniques and continue to be widely used. Most devices utilize firewalls or associated tools to monitor traffic and mitigate threats.

10. Social engineering or insider threat:

Social engineering is a manipulative technique which uses human error for the purpose of obtaining access, personal information, or valuables. In cybercrime, "human hacking" scams tend to attract unsuspecting users to expose data, spread malicious software infections, or give restricted systems access.

Conclusion

Cyber security is one of the most important aspects of the fast-paced growing digital world. The threats of it are hard to deny, so it is crucial to learn how to defend from them and teach others how to do it too. If you want to learn more about what is cyber security and how to deal with cyber criminals hop into our **courses section** and become a hero in the digital platforms.

Reference- Yash

arya sir