Cyber security Approach for Programs and Networks

Zina Mohamed Salih
University of Kerbala , Kerbala, Iraq
Zina.mohamed88@gmail.com

Abstract

It is the process of protecting systems, networks, and programs against digital attacks. These cyber attacks usually aim to access, alter or destroy sensitive information; For .the purpose of extorting money from users or interrupting normal business operations Implementing cyber security measures is a huge challenge today because there are more devices than people and attackers are becoming more innovative. A successful cyber security approach has multiple layers of protection spread across computers, networks, programs or the data one wants to preserve. People, processes and technology must complement each other within an organization to create an effective defense against cyber attacks .

A unified threat management system can automate integrations across selected CiscoSecurity products and accelerate the functions of key security operations detection, investigation, and remediation.

Introduction

Persons

Users must understand and comply with basic data security principles such as choosing strong passwords, being wary of email attachments, and backing up data. Learn more about the basic principles of cyber security

Processes

Organizations must have a framework on how to deal with incomplete and successful cyber attacks. One respected framework can guide you. Shows how you can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks. Watch the video explanation of the NIST Cyber security Framework

Technology

Providing technology is essential to giving organizations and individuals the necessary cyber security tools to protect themselves from cyber attacks. Three main entities must be protected: peripheral devices such as computers, smart devices and routers, networks, and the cloud. Common technologies used to protect these entities include next-generation firewalls, DNS filtering, anti-malware protection, antivirus .software, and email security solutions

cyber security roll in programs protection :

In today's connected world, everyone benefits from advanced cyber defense software. On an individual level, a cyber security attack can result in a lot of things, from identity theft to extortion attempts to the loss of important data like family photos. Everyone depends on critical infrastructure such as power plants, hospitals, and financial services companies. Securing these and other institutions is essential to keeping our society functioning

Everyone also benefits from the work of cyber threat researchers, such as the Talos team of 250 researchers, who investigate new and emerging threats and cyber attack strategies. They work to expose new security vulnerabilities, educate the public about the importance of cybersecurity, and support open source tools. Their efforts make the .Internet a safer place for everyone

Types of cybersecurity/phishing threats

Phishing is the process of sending fraudulent emails that look like emails from trusted sources. The goal is to steal sensitive information such as credit card numbers and login information. It is the most common type of cyber attack. You can help protect yourself with education or by using technical solutions that filter malicious email .messages

Malware :

Ransomware is a type of malware. It is designed with the aim of extorting money by blocking access to files or a computer system until the ransom is paid. Paying the .ransom does not guarantee file recovery or system recovery

Cyber security strategic roadmap

A cyber security strategy creates a coordinated strategy that responds dynamically to threats to national security. One manifestation of this emerging national security threat is the national exposure to risks from the uncoordinated presence in cyberspace. In the context of immediate and future security challenges, the National Cybersecurity Strategy for Iraq aims to manage security threats in cyberspace in line with the goals of general national security and the public interest. Whereas the national vision for cybersecurity is directed towards a safe, secure, vibrant, flexible and reliable society that provides opportunities for its citizens, protects national interests, promotes peaceful interactions and proactive participation in cyberspace for the sake of national .prosperity

The vision also aims to strengthen national capabilities in the field of cyber security in Iraq in a coordinated, sustainable and integrated manner in order to address and mitigate cyber risks in cyberspace and reduce its severity. The national cyber security strategy aims to protect the national information infrastructure in various fields, and for this purpose, the areas that must be worked on must be identified in a coherent executive framework to raise the level of cyber-Iraq towards a safe cyber environment. It will also shed light on the ways in which early warning, detection, interaction and crisis management will be evaluated, developed and implemented to provide proactive readiness to respond to and deal with threats to critical information .infrastructures in Iraq

Where the Iraqi Electronic Response Team (CERT) began its tasks in this regard and worked to find measures and procedures to bridge the cyber security gap and address its basic weaknesses. The Iraqi Electronic Response Team (CERT) also formed several teams working separately and in a coordinated manner, where the areas that must be worked on were divided and classified in a way that guarantees the productivity of the Iraqi cyber security strategy and within a specific time frame into sections and according to the international standard of the International

Telecommunications Organization (ITU) As well as to ensure the upgrading of the level of cyber Iraq .

Refrences :

1- Ross J. Anderson: Security Architecture: A Guide to Building Reliable Distributed Systems, ISBN 0-471-38922-6
2- Maury Jacir: Building a Secure Computer System. ISBN 978-0-442-23022-2 1988
3- Stephen Haag, Maeve Cummings, Donald McCabery, Alan Pinsonalt, Richard Donovan: Managing Information Systems for the Information Age, ISBN 0-07-091120-7
4- J. Stuart Lee: Essays on Computer Security Cambridge, 1999
5- c. Peter Neumann: Trustworthy Associated Architectures with Principles 2004
6- Paul A. Cargire, Roger R. Shell: Thirty Years Later: Lessons from the Multics .Security Assessment, IBM White Paper
7- Bruce Schneier: Secrets and Lies: Digital Security in a Networked World, ISBN 0-471-25311-1
8- Robert C. Secord: Secure Cryptography in C and C++. Addison Wesley, September 2005. ISBN 0-321-33572-4
9- Clifford Stoll: The Cuckoo's Egg: Tracking and Spying Through a Labyrinth of Computer Espionage, in Pocket Books, ISBN 0-7434-1146-3