International Journal of Innovation in Computer Science and Information Technology
Vol.3, NO.4 , P: 72 - 81
Received : 18 September 2021
Accepted : 12 October 2021

Requirements of Secure Architecture for Computer Systems

Shima Goodarzi*
MA Student, Department of Computer Engineering, Faculty of Electrical and Computer Engineering, Islamic Azad University, North Tehran Branch, Tehran, Iran
Shimagoodarzei@Gmail.Com
Dr. Naser Modiri
Department of Computer Engineering, Faculty of Engineering and Basic Sciences, Islamic Azad University, Zanjan Branch, Zanjan, Iran
Nassermodiri@Yahoo.Com

Abstract

Expansion of information technology and the larger dependence of organizations' operations on it have resulted in the increased security threats; hence, to maintain operations, protect assets and business continuity, cybersecurity is necessary and part of the inevitable costs of organizations. There are numerous approaches to protect cybersecurity. Preventive defense is one of the significant approaches in cybersecurity, protecting the information of the organization and as one of the important organization's survival pillars.

The present paper investigates and assesses a set of Reference Architectures [2] as well as commonly used models in cybersecurity, presenting a new and agile model according to the best practices of each model so that given the severity and extent of the current changes, it may rapidly respond to the organization's security needs, including the NIST framework [1], cloud computing, cloud computing security, threats and threat solutions.

Keywords: Network Security Architecture, Cyberspace Threats, Cyber Security, Cyber Vulnerability

Introduction

Architecture refers to a structured definition or solution that may meet all the expected technical and operational needs. Our main approach is SRA (Security Reference Architecture). It is very important for successful acceptance and security to know the various security options and how to apply them in the solution [2].

This architecture indicates an overview of security components for secure deployment, development, and operation. The Cyber Security Reference Architecture (SRA) describes cybersecurity capabilities as well as the way they integrate with the current architectures and security capabilities. This architecture may be employed to establish cybersecurity by organizations' internal teams.

The starting pattern for security architecture is that the organizations use a template to help define the target state for establishing cybersecurity. Organizations consider this architecture helpful since it includes the capabilities of the organization.

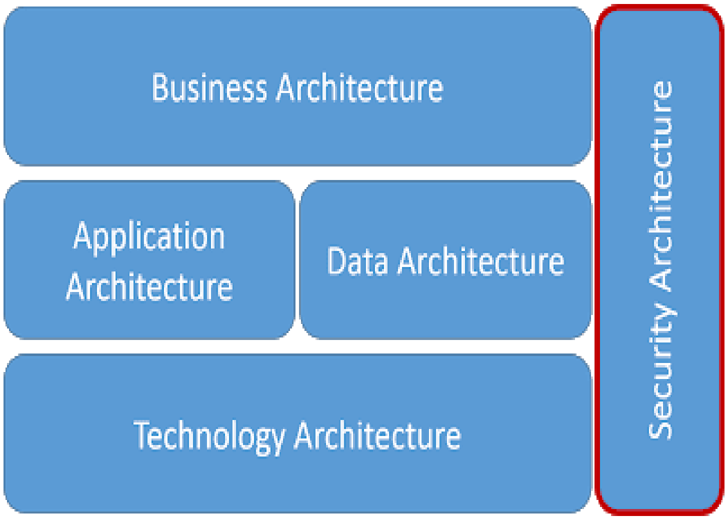


Fig. 1 shows the Cyber SRA, which may be utilized by organizations' internal teams to establish cybersecurity.

The NIST reference model is the most significant reference model for the computer systems' secure architecture, consisting of five steps below [1]:

1. Defining targets: Before thinking about implementing NIST, the objective of this implementation should be determined.

2. Preparing an accurate profile: The next step is to test run that Framework more specifically to meet the organization's particular needs.

3. Assessing the current situation: After the above steps, it is significant to accurately conduct the risk assessment, so that a specific situation may be created.

4. Analyzing the difference between the results and identifying the necessary actions: The gap between the results may be analyzed by knowing the cybersecurity risks and potential business effects for the organization.

5. Implementing an operational plan: With a clear picture of the validity of the present cybersecurity defense, a set of organizational objectives, a comprehensive analysis of the gap between actual and expected outcomes, as well as a set of corrective actions ultimately result in the desirable implementation of NIST CSF.

Confidentiality
Integrity
Data Security
Availability

Secure Architecture's Specifications:

1. **Confidentiality**: The information sent between the sender and the receiver is confidential and no one will be informed about that.
2. **Integration**: In many applications of the network, we may want to send data from source to destination that is no longer a secret; however, it is important that no one may modify or falsify this data.
3. **Accessibility**: This objective is related to the server. The server must always be available since profiteers may attack it; thus, to prevent them, the server should have a mechanism against the attacks. Intrusion detection is a most widely used method.

In general, 40% of technology plays a role in security and 60% of security modems cannot be measured and we can only announce how insecure we are nons = nonciA.

Defense: It is a set of measures taken to protect information against or for repelling aggression.

Security: It stands for the protection provided to an automated information system for effectively protecting the information system resources' accessibility and confidentiality.

The difference between defense and security: Security refers to a precautionary measure, but defense means knowing the methods and tactics for opposition.

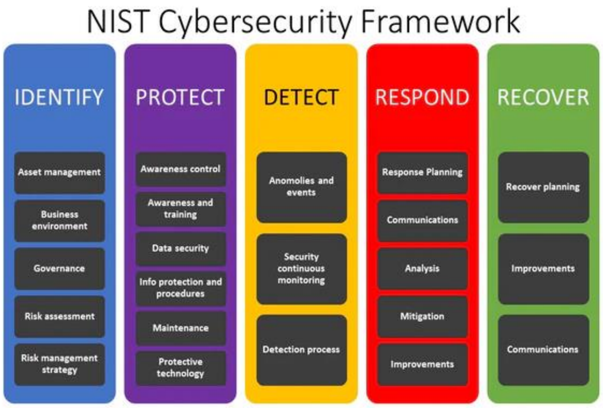
Architecture: It is how modules are placed side by side and complemented to make a framework.

Model: It refers to simplifying the system for better understanding [3].

NIST Framework:

The first version of the cybersecurity framework was released for providing guidance to organizations willing to strengthen cybersecurity defenses. Although most organizations have found the importance of strengthening cybersecurity defenses, in practice, this joint effort to improve cybersecurity across all organizations and implement this framework is very difficult.

The following figure exhibits the cybersecurity framework in NIST, published to provide organizations seeking to strengthen cybersecurity defenses with guidance.



The most important reference model for the secure architecture of computer systems is the NIST reference model, which consists of 5 steps.

NIST Reference Model
Defining targets: Before thinking about implementing NIST, the objective of this implementation should be determined.
Preparing an accurate profile: The next step is to test run that Framework more specifically to meet the organization’s particular needs.
Assessing the current situation: After the above steps, it is significant to accurately conduct the risk assessment, so that a specific situation may be created.
Analyzing the difference between the results and identifying the necessary actions: The gap between the results may be analyzed by knowing the cybersecurity risks and potential business effects for the organization.
Implementing an operational plan: With a clear picture of the validity of the present cybersecurity defense, a set of organizational objectives, a comprehensive analysis of the gap between actual and expected outcomes, as well as a set of corrective actions ultimately result in the desirable implementation of NIST CSF.

Categories of NIST Framework Method(table1)

Category	Unique class ID	Function	Unique performance ID
Asset Management Business environment Government Risk Assessment	ID.AM ID.BE ID.GV ID.RA ID.RM	Identifying	ID

Risk Management Strategy Supply Chain Risk Management	ID.SC		
Identity Management and Access Control Awareness and Education Data Security Steps and Methods of Information Protection Maintenance Security Technology	PR.AC PR.AT PR.DS PR.IP PR.MA PR.PT	Protection	PR
Abnormalities and Events Continuous Security Monitoring Detection Processes	DE.AE DE.CM DE.DP	Discovery	DE
Response planning Communications Analysis Decrease Advances	RS.RP RS.CO RS.AN RS.MI RS.IM	Responding	RS
Recovery planning Advances Communications	RC.RP RC.IM RC.CO	Recovery	RC

Identification step in cyber preventive security assessment tool(table2)

Near goals (third stage)	Near goals (second stage)	Near goals (first stage)	Goals	Category	Function
3	2	1	3	Asset Management	Identifying)ID(
2	1	0	2	Business environment	
3	2	1	3	Government	
3	2	1	3	Risk Assessment	
2	1	0	2	Risk Management Strategy	

3	2	1	3	Supply Chain Risk Management	
2.7	**7.1**	**7.0**	**7.2**	**Average (ID)**	

Protection step in cyber preventive security assessment tool(table3)

Near goals (third stage)	Near goals (second stage)	Near goals (first stage)	Goals	Category	Function
3	2	1	3	Access Control	Protection)PR(
2	1	0	2	Awareness and Education	
2	1	0	2	Data Security	
2	1	0	2	Steps and Methods of Information Protection	
2	1	0	2	Maintenance	
2.2	**2.1**	**2.0**	**2.2**	**Average (PR)**	

Detection step in cyber preventive security assessment tool(table4)

Near goals (third stage)	Near goals (second stage)	Near goals (first stage)	Goals	Category	Function
2	1	0	2	Detection Processes	Detection (DE)
2	1	0	2	Abnormalities and Events	
3	2	1	3	Continuous Security Monitoring	
2.3	**1.3**	**0.3**	**2.3**	**Average (DE)**	

Responding step in cyber preventive security assessment tool(table5)

Near goals (third stage)	Near goals (second stage)	Near goals (first stage)	Goals	Category	Function
3	2	1	3	Detection processes	Respondse (RS)
2	1	0	2	Response planning	
2	1	0	2	Response Communication	
2	1	0	2	Accident analysis	
2	1	0	2	Accident reduction	
2.2	**1.2**	**0.2**	**2.2**	Average (RS)	

Recovery step in cyber preventive security assessment tool(table6)

Near goals (third stage)	Near goals (second stage)	Near goals (first stage)	Goals	Category	Function
2	1	0	2	Accident investigation	Recovery (RC)
3	2	1	3	Recovery planning	
4	3	2	4	Recovery improvements	
4	3	2	5	Recovery Communications	
3.3	**2.3**	**1.3**	**3.3**	Average (RC)	

Cloud Computing

In computing history, the cloud computing evolution over the past few years is potentially one of the major advances. Nevertheless, in case that cloud computing reaches its potential, there must be a clear understanding of the various involved issues, both from the viewpoint of technology providers and consumers. While much research is now being conducted on technology itself, there is an urgent need to recognize the business issues of cloud computing. In the present paper, the strengths, weaknesses, opportunities, and threats of the cloud computing industry are identified. The various issues that will affect different stakeholders of cloud computing will be then identified [4].

Cloud Computing Security

Cloud computing refers to a distributed architecture concentrating the server resources on a scalable platform in order to provide the on-demand computing resources and services. It has become a changing platform for companies to construct their infrastructure. If companies want to apply cloud systems, they must seriously re-assess their present security strategy and specific aspects of the cloud that need to be assessed [5].

Threat Modeling

Pre-attack reinforcement and prevention is the fundamental part of a system's security, since often post-attack defense cannot be very effective. The important thing in the **world of network security** is to consider (how), not just (who), and in simpler and more important terms, how a cyber theft occurs, not who performs it. The focus in threat modeling is on how the attack occurs and results.

Threat modeling refers to a way to optimize system security made possible through identifying targets, intrusion methods, as well as vulnerabilities. The first and fundamental step in threat modeling is to identify all the things we want to protect.

- STRIDE

It stands for a threat model run to help investigate and identify potential threats to a system. The STRIDE method is employed to ensure that a program is in line with the CIA (confidentiality, integrity, and availability) Security Guidelines, besides authentication, licensing, and non-denial of spoofing, tampering, repudiation, information disclosure, denial of service (DoS), and elevation of privilege. The abovementioned show six groups of threats, each of which violating a specific feature of the system from the CIA's three changes.

Fig. A-5. presents six groups of STRIDE threat. Threat modeling allows security aspects and software developers to deal with the inevitability of hackers trying to compromise a system at the beginning of a project life cycle [6].

- DREAD

It is a type of quantitative risk analysis including grading the severity of cyber threats. The DREAD model declines the previous damage and may provide greater safety in the future. The key points of cyber threats should be assessed in this method, while a numerical rating is given to each of these points. After completion, the overall ranking may be compared to the DREAD model rating system that should indicate the low, medium, or high risk of cyber threat to the business.

To assess the severity of cyber threats, five key points must be scrutinized when using the DREAD model and they should be then scaled to one, two, or three. A rating of one shows low risk. A ranking of two stands for a moderate risk. A ranking of three refers to a high risk [6

Att & ck

Att & ck concentrates on network defense, describing the operational stages of the life cycle, before and after an enemy's operation; for instance, they use stability, lateral movement, explosion, as well as the details of specific tactics, techniques, and methods (TTP) that progress continuous threats (APT) to reach their goals when targeting, compromising, and working within the network.

Cyber Criminology Methods

The following are five of the fundamental cybercrimes related to businesses and individuals in 2020:

1. Phishing Scams

According to the PhishMe study, most successful cyberattacks - 91%, - begin when curiosity, fear, or a sense of personal urgency prompts someone to enter personal information or click on a link.

Phishing emails mimic the messages of a person or business you know or trust. They are designed to trick people into entering the personal information or clicking on malicious links downloading malware. Thousands of phishing attacks happen daily.

2. Website Forgery

The word forgery means fraud or deception. A website forgery occurs when a website is designed in an actual form, deceiving you that it is a legitimate site. This is conducted to gain your trust, access your systems, steal data, steal money, or spread malware. Through duplicating a legitimate website with the style, brand, user interface (UI), and even domain name of a large company, website forgery seeks to trick users into entering their usernames and passwords. In this way, bad people will record your information or install malware on your system.

3. Ransomware

Ransomware refers to a modern technique for a crime existed for a long time – extortion/exaction. At its core, ransomware is applied when criminals steal something valuable and demand payment. For most businesses, this includes encrypting the company data. With the emergence of ransomware, jobs are at a standstill and employees cannot perform their works.

4. Malware

Norton defines malware as “destructive software” specifically designed to access or damage a computer/system. While ransomware is designed to hold your data hostage, it is not the only type. There may be numerous objectives for malware - power, intrusion, money, information – however, the result is always the same - an effort to a time-consuming and often expensive recovery.

5. IoT Hacking

The Internet of Things (IoT) is a brave bold new world opening up our daily insights and workflows to the web. Whether we like it or not, all these Internet-connected objects are collecting and exchanging information. As you know, data is of great value; accordingly, hackers try to exploit any device collecting it [7].

Conclusion

Various architectures have been presented to secure cyber systems, each outlining its methods, strategies, and programs through emphasizing aspects of security. The present paper assesses the NIST model as one of the most widely used reference models, presenting the most important criminological methods, threats, and features of a secure architecture, cloud computing, and cloud computing security.

References

1. https://www.nist.gov/cyberframework

2.https://www.interstell.com/wordpress/security-reference-architecture-the-wheel-does-not-need-reinventing/

3. https://attack.mitre.org/

4. T. Alford, G. Morton, The Economics of cloud computing, Booz Allen Hamilton, 2009.

5. Mather, T., Kumaraswamy, S. and Latif, S. (2009) Cloud Security and Privacy, O'Reilly, ISBN. 978-0-596-80276-9

6. Proactively Detect Persistent Threats Cyber Kill Chain, [online] Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. (20 December 2020, date last visited).

7. www.springerprofessional.de