Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 8, S. 172-182, 5, 2024

Araştırma Makalesi

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 8, pp. 172-182, 5, 2024

Research Article

https://as-proceeding.com/index.php/ijanser
ISSN: 2980-0811

Importance of Information and Network Security: Evaluation within the Scope of Business

Ayşenur ERDİL[*] [1]

[1] *Faculty of Political Sciences, İstanbul Medeniyet University, Turkey*
[*] *runesyalidre@gmail.com - ORCID ID: 0000-0002-6413-7482*

(Received: 23 June 2024, Accepted: 27 June 2024)

(3rd International Conference on Frontiers in Academic Research ICFAR 2024, June 15-16, 2024)

ATIF/REFERENCE: Erdil, A. (2024). Importance of Information and Network Security: Evaluation within the Scope of Business. *International Journal of Advanced Natural Sciences and Engineering Researches*, 8(5), 172-182.

Abstract – From past to present, security has played an important role in every aspect of life. With the rapid development of computer technology, different problems and solutions have emerged in the field of security. Previously, organizations and companies only had their own local networks, but due to the need for communication between these organizations, networks have expanded further and security has become very important in parallel. Security has emerged to prevent external attacks or damages caused by user errors on these computer networks, wired, wireless networks and the internet used by organizations. Wireless networks provide significant advantages thanks to various benefits such as easy use and flexibility. However, they also have several disadvantages compared to a wired network. Security risks are at the top of these disadvantages. In order to ensure that the security of this network, which emerges entirely from the requirements, is provided correctly, it is necessary to evaluate, analyze and analyze the information security risks of network policies. This analysis and evaluation is done according to certain criteria. Accordingly, in this research, in the light of these criteria, evaluations, network security policies, determination and analysis of information security risks related to security policies are included in the direction of providing network security for businesses and institution

Keywords – Business, Information Security, Security network

I. INTRODUCTION

An examination of the network and all of its elements, including performance, security protocols, infrastructure, and more, is called a network assessment. This procedure generates a report called a network assessment, which provides you with an overview of all the activities occurring on your network, including devices that are connected and users, available bandwidth, traffic from users patterns, and problems that require attention. An evaluation is an excellent tool for entrepreneurs who do not possess a complete understanding of their Technology setup and need clarification, or who are thinking about improving their current network. Enlisting the services of a provider of Information Technology (IT) services to do this task is especially beneficial for organizations that lack this competence in-house. A third party may conduct an objective and thorough analysis of your systems, utilizing their deep technological knowledge to give you with the most efficient recommendations (Levy et al., 2007; Network Security Assessments, 2024; Network Infrastructure What Is a Network Security Assessment, 2024).

A network security policy establishes who is allowed access to and removal from the network. It may restrict the types of data that may move from private to open networks and internet-based material that internal users could view. Traditional computer networks and wireless networks share many of the same concepts when it comes to security. Wired and wireless networks share many infrastructure-related themes that are applicable to a wide range of operations. One essential component of network security is having a strong policy for network security. The components of a complete security policy—both technological and conceptual—are covered in this chapter. The aforementioned elements range from user authentication techniques to hardware to human procedures for interacting with wireless devices. Implementing the physical elements and their software alternatives is crucial in a network security strategy, as is improving staff behaviors and fundamental security awareness via effective training. Even occurrences that an administrator of networks is unable to avoid may be properly prepared beforehand. The principles presented in the following paragraphs offer the user with a good foundation for developing a customized wireless network security strategy. In order to guarantee the safety and security of a company's networks, devices, and data, network security evaluations are essential. These evaluations assist in locating possible avenues of entry for external and internal cyberattacks. Organizations may proactively build their defenses and guard against potential dangers by assessing prospective assaults. A network security assessment often consists of inventorying an organization's resources, establishing the worth of information, analyzing the vulnerability of the IT infrastructure, testing defences, and recording the findings in a report. This approach assists companies in assessing their security posture and identifying opportunities for improvement. It is critical to remember that network security assessments are a continuous process that must be carried out on a frequent basis in order to keep ahead of developing threats (Levy et al., 2007; Network Security Assessments, 2024; Network Infrastructure What Is a Network Security Assessment, 2024; How to Accurately Define the Scope.., 2024).

The scope of work entails determining who, what, and how technology, processes, and people interact with or could affect the confidentiality of the data that has to be safeguarded. One of the most crucial parts of a data security evaluation is the scoping phase, which is the initial stage in any evaluation. If any pertinent individuals, procedures, or technologies are overlooked, it might negatively affect the evaluation's overall quality and dependability. A formal written declaration outlining a plan for managing every aspect of a computer network that pertains to network security is, in essence, a network security policy.

Organizations have built their own computer networks by linking their computers in a variety of ways in response to the requirement to share resources and information. These networks have subsequently been modified to connect to the Internet in order to facilitate communication with external parties.

With the advent of settings like networks of computers and the Internet, the idea of security—which was formerly achieved by closed rooms—has taken on new meaning. Laws are unable to regulate the imaginary world that is the Internet. Attackers attempt to obtain information illegally in this virtual environment by taking advantage of network vulnerabilities. In addition to being compromised by assaults, a great deal of information gets lost or has its content altered as a result of users' careless mistakes. Organisations may suffer from both monetary and moral losses, such as a loss of confidence. It is necessary to establish certain regulations in order to handle such circumstances (Levy et al., 2007; Liu et al., 2016; Network Security Assessments, 2024; Network Infrastructure What Is a Network Security Assessment, 2024; How to Accurately Define the Scope.., 2024).

A range of security rules are implemented by network operators to safeguard the information and services. Nevertheless, since conventional networks have dispersed network control and no common control protocol, implementing these regulations is challenging and security-vulnerable. A software-defined network, which separates the control layer from the data plane and takes use of conceptually centralized management, offers an appropriate model to handle these issues. In this work, the developers emphasize about utilizing networking that is software-defined to enforce security standards. In order to implement security rules, researchers suggest a two-layer OpenFlow switch topology that takes into account the flow table size limit on a single switch, the difficulty of assigning safety regulations to these types of switches,

and the load balancing between these switches. Moreover, it offers a secure updating method (Liu et al., 2016; Network Security Assessments, 2024; Network Infrastructure What Is a Network Security Assessment, 2024).

Encouraging the widespread adoption and deployment of new security features and protocols on the Internet has been an ongoing challenge. This is due to a number of factors, chief among them being economic ones brought on by network externalities. In fact, the technologies used to safeguard the Internet exhibit network effects, meaning that their worth varies depending on whether other users choose to adopt them or not. Specifically, the advantages seen by early adopters of security solutions may be far less than the adoption costs, which makes it challenging for those solutions to become popular and be widely implemented. In this study, researchers aim to quantify and predict the effects of these externalities on the uptake and implementation of security features and protocols (Lelarge and Bolot, 2008).

The present study examines security choices made by identical plant-controller systems when network-induced threats cause their security to be interdependent. A discrete-time stochastic linear system is used to describe each plant, and the systems are managed via a common communication network. We frame the issue of system operators' (also known as players') individual security decisions as an uncooperative game. Researchers consider a two-stage game where players use control inputs to minimize average operating expenses in the second stage, after deciding whether or not to invest in security in the first. They identify the game's equilibria, which involves figuring out each player's ideal security level. They then resolve the issue of determining the security levels that are socially optimum (Heal and Kunreuther, 2003; Amin et al., 2013). Most pipeline security approaches are either qualitative or semi-quantitative, depending on expert opinion and hence perhaps subjective. The present research offers a novel approach to security vulnerability evaluation, utilizing the Discrete-time Bayesian network (DTBN) technique to examine the vulnerability of a pipeline, which is considered a hazardous facility, while taking security countermeasures into account. The approach is used to rank order the pipeline segments according to their criticality in an example gas pipeline (Fakhravar et al., 2017).

Nowadays, policy-driven managing is becoming more and more common, mostly because massive networked systems are becoming more and more sophisticated and large in scale. Policies are typically employed in these types of systems to streamline system administration activities and allow for future system expansion. As a result, many policy languages are put out to communicate administrators' objectives in policy-driven systems, particularly in relation to network and security management. As a result, this article examines recent efforts, highlights important concerns, and finally describes the work that policy languages will be doing in the coming years (Han and Lei, 2012). Networking security policies are made through putting in writing the basic guidelines for the proper utilization of resources on networks that companies have built and modified for the Internet, as well as the regulations for network configuration. A security policy's most crucial component is its written form, which outlines in detail how every person in the Company from the end user to the administrator will utilize the company's information assets and technology. Network security policies have to be established, if at all feasible, prior to the installation of the system and before security problems arise. Making a security measure for a system that has been set up is additionally less complicated than this. It is impossible to create a safe computer network lacking a security policy (Levy et al., 2007; Lelarge and Bolot , 2008; Liu et al., 2016; Network Security Assessments, 2024).

II. Materials and Method

Network safety procedures are critical for protecting organizational resources and guaranteeing the safe and correct use of the network's components. These policies define an arrangement for controlling and safeguarding network assets, directing users, and ensuring network reliability.

A. Network Security Policy

One cannot discuss a model for network security rules since they differ based on the needs and organizational structure. The factors to be taken into account while drafting a security policy are discussed

in this research. Several sub-policies can be discussed while discussing details and network security regulations. This is a result of subject- or technology-specific regulations. The following is a list of fundamental policies needed to guarantee the safety of networks. These are; Policy for military security, Policy for commercial security, Statement of Privacy, The policy of reliability, Policy on Acceptable Use, Policy for Access, Policy for network firewalls

Internet guidelines, Policy for managing passwords, Policy for physical security, Policy on social engineering. The definitions of these concepts of networks security policy are below (Stallings, 2002; Levy et al., 2007; Lelarge and Bolot, 2008; Network Infrastructure What Is a Network Security Assessment? 2024).

Policy for military security: Privacy is the primary goal of such policies. Privacy remains foremost, but accessibility and reliability are equally crucial. While it is possible to overcome the other two, there are serious repercussions for violating confidentiality. Think about the confidentiality of a military ship's time of departure, for instance. By sending this information by hand, security and accessibility issues can be resolved in this situation. This makes the information dependable and easily available. If enemies were to intercept this information, the repercussions would be even severe.

Policy for commercial security: Reliability is the primary goal of this type of strategy. The term *"commercial"* refers to the fact that the objective of applications for business is to prevent data manipulation. For instance, a bank would be embarrassed and the customer would choose to utilize another bank if confidentiality was compromised and user account information was made public. On the other hand, there is a serious financial issue if accounts of users are compromised. Consequently, in these kinds of applications, dependability is the most crucial factor.

Policy on Acceptable Use: The proposed policy ought to address the following and related matters: - Who can utilize the resources?; - How can resources be used appropriately?
- Who has the authority to approve usage and allow access?; - Who is eligible to set management priorities?, -What could be performed with confidential data; - What have been the privileges and duties of users; - What are the privileges and duties that lie with system managers toward consumers.

Statement of Privacy: This policy's only goal is confidentiality. This is different from military security strategy in that there are other goals in addition to secrecy as the main goal.

The policy of reliability: As with the privacy policy, this policy's only goal is dependability.

Policy for Access: The permissions granted to individuals for connecting to the network are determined by accessibility policies. The permission granted to each user to access the network need to vary. Once users have been classified, access regulations have to be decided upon individually for each group. These categories also include system administrators. Some system restrictions ought to be left up to the system administration's discretion if restrictions on access have not been established specifically for the administrator of the system. This might result in unintended security flaws on the system.

Policy on social engineering: The practice of getting knowledge about a person and convincing them to perform what someone desire is referred to as social engineering. One approach is to physically enter the company under the pretext of a technician, attempt to obtain the user's passwords through pretending to be the systems manager, or gather information through searching through trash cans. Workers for the company should always keep their personal and professional lives apart and never give information to anybody who cannot verify their identification. The company's rules should include any required precautions and precautions about such circumstances.

Policy for network firewalls: In order to address issues which a business might encounter with its Internet connection, a firewall on the network serves as a gateway separating its internal network and external networks. This is where access control is applied for network connections from outside to within. As such, it runs concurrently with access policies. In addition to defending the system from outside threats, firewalls are also used to improve performance and enforce authorization policies. Software or hardware with software integration can be used as such solutions. Firewall user interfaces may be used to establish access rules that follow the policies of the company. Safety for networks may be achieved using firewall in conjunction with the subsequent Technologies (Bace and Mell, 2001; Stallings, 2002; Levy et al., 2007;

Lelarge and Bolot, 2008; Cárdenas et al., 2008; Network Security Assessments: Importance and Best Practices, 2024; Network Infrastructure What Is a Network Security Assessment?, 2024).

(i) Proxy: A proxy server is an application that acts as a middleman between an end user and the connection deployment, performing the connection effectively. An application-level firewall is another name for using a proxy. This kind of application is also used to manage access to these applications and optimize bandwidth use for optimal performance.

(ii) Technologies that scan HTTP, FTP, and SMTP communications for viruses and remove them before they reach users are known as anti-virus solutions.

Systems which scrub websites and emails that arrive so that different applications can access them are known to be monitoring systems.

(iii) Virtual private networks (VPNs), or VPNs for short, are used to improve the reliability of business network connections across public data networks. Using a public/private key ensures that the data being transferred is encrypted. Tighter policy definitions are required when the quantity of components utilizing VPN rises.

(iv) Systems called intrusion detection systems (IDS) are designed to identify unusual activity, hacking attempts, and assaults. When something seems suspect, IDS can notify a system administrator by email or mobile device.

The safety precautions ought to be followed while configuring each of these offerings and deciding which rules to employ.

Businesses' increasing information technology (IT) security spending demonstrate the importance of IT security to them. To control IT security concerns, businesses rely on security solutions like intrusion detection systems (IDSs) and firewall. The usefulness of these technologies is a topic of contention in the IT security community, despite the abundance of scholarship on the technical elements of IT security. Everyone wants to evaluate the usefulness of IDSs in an organization's IT security architecture in this article. We discover that whether a company achieves a positive or negative outcome from the IDS depends on the setup of the system, as indicated by the rate of detection (true positive) and alarming (false positive) rates. In particular, we demonstrate that an IDS yields a positive outcome for a company only if its detection rate is high (Bace and Mell, 2001; Stallings, 2002; Levy et al., 2007; Lelarge and Bolot, 2008; Cárdenas etl., 2008; Network Security Assessments: Importance and Best Practices, 2024; Network Infrastructure What Is a Network Security Assessment?, 2024).

Internet guidelines: Every worker in a company has to have access to the Internet or other external resources. The following are some issues that Internet access may bring about:

Misuse: The Internet connection may be abused by using it for objectives unrelated to the company. Large data downloads from the Internet, including music and movies, would inevitably overload the line's capability and might slow down the rate at which external resources can be accessed.

Active Code: Applications that may travel the web thanks to Active Code, like Java and ActiveX, may also be used for malicious reasons. While Java's control mechanisms can help avoid some of these attacks, ActiveX does not have the same protections. Because of this, the Internet browser's parameters for using these codes need be adjusted

Virus-ridden codes: It is possible for malicious software, such trojans or viruses, to infiltrate the system. Each user's computer has to be configured to install antivirus software and enable Internet (http, email, ftp) functions, such as analyzing server traffic and sending the user's content once it has been cleaned, in order to defend against viruses.

It is possible to take action. The firewalls have to be hardened to prevent the employment of Trojan horses, which could result in security flaws in the system.

The company should specify which external users partners, customers, workers, and others have permission to utilize business network resources and to what level of exposure.

Policy for managing passwords: Using passwords as a control mechanism, researchers can determine if individuals are authorized to access the data they desire. Since improper or fraudulent password use may result in security issues, passwords play a crucial role in security policy. When required, system administrators should step in and influence users' password selections. Users ought to be informed, tools

should be used to identify weak passwords, and consumers should be cautioned in order to deter users from using straightforward and easy passwords. Every account should have its own password, which should be updated on a regular basis. Users should notify authorised entities and take appropriate action if they believe their credentials have been compromised. The following subsection provides comprehensive details on passwords selection and usage. The user's duty is not finished during passwords selection; any password may be broken given enough time and resources.

(i) *Single Sign On (SSO) policy making:* The user has access to all network apps for which they are authorized with just one password. End consumers will benefit from this as they won't have to keep track of numerous passwords all at once.

(ii) *Policy on expiration of the password (obsolescence):* Users are compelled to create new passwords since their current ones are no longer valid. By doing this, a username and password control system is established.

Policy for physical security: It ought to be mentioned that a hacker may quickly take over a computer or other active device if they have physical access to it. If an attacker gains access to the network connection, they can use specialized equipment (tapping) to access the cable and use it to transmit or receive messages. It should be made very evident that installing software security measures on an unsecured computer is pointless. The company should decide on physical safety precautions that might be implemented for the computer systems that host services and the primary devices that comprise the network.

B. Application Layer Security/IDS

It is not possible to completely secure poorly designed networks using techniques like encryption and intrusion authentication. For instance, the suggested fixes are insufficient when it comes to rogue nodes negotiating mutual concessions. The system requires an additional line of defence. An intrusion detection system, often known as an intrusion detection system (IDS), is a device that sounds an alert when it notices unusual activity on the network. Systems for detecting intrusions continually scan the network for strange activity. The system's primary source of information is accumulated audit data, which it uses to detect and react to hostile behaviours directed at network resources. This data may be kept momentarily for an ongoing procedure or permanently for use at a later time. Configuration options govern where and how data is gathered as well as how to handle breaches. Intrusion detection systems only have access to the traffic that is currently entering and leaving the node in ad hoc networks without centralized control points like routers. The distributed nature of the algorithms these systems employ is another essential prerequisite. It also has to be considered that a node can only observe a portion of the network. Specifically, the network It is conceivable for one or more of the nodes to be hacked if they are discovered in an aggressive environment. It is questionable which nodes may be trusted if the intrusion detection systems' algorithms cooperate. Consequently, with ad hoc networks, it's important to be on guard against both external and internal threats (Stajano and Anderson, 1999; Zhou and Haas, 1999; Stallings, 2002; Yang et al., 2004; Levy et al., 2007).

C. Determining the Needs of the Organization

Deciding which organizational requirements this policy ought to be established for should be the initial phase in creating security policies. The following actions need to be completed in order to draft the policy (Stallings, 2002; Levy et al., 2007; Cárdenas et al., 2008; Network Security Assessments: Importance and Best Practices, 2024; Network Infrastructure What Is a Network Security Assessment?, 2024):

- Determining what has to be safeguarded: This may involve non-computer related textual materials that are extremely important to the company, as well as computer resources like software and hardware. Identification of servers and communicating devices is important for safety of networks. It ought to be made sure that the unit in charge of network security receives information via request, including who and what services the servers' offering goods and services over the network offer, the protocols they employ, and the email address and phone number of the admins who oversee these servers. Each unit's local system administrators who oversee its computer operations should be reached through phone, formal letter, or both, and server information ought to be gathered. Traffic through the network monitoring might also yield undelivered information.

- Choosing the target audience for the protection: This should be done by considering all scenarios in which the resources that need to be safeguarded may be harmed. These might be individuals who launch attacks from within the company or over the Internet.
- Develop the information storage strategy: Businesses must decide how to store and transfer information. For instance, all information might be communicated informally in one organization but formal correspondence would be required in another.
- Information backing and conserving: In order to reduce data loss, organizations should archive their old data and keep it accessible for future use. Regulations should specify what sort of data ought to be stored up, how frequently backups should happen, and who would do the backups.
- Establishing roles throughout the organization: It is important to ascertain the workers' areas of accountability as well as their roles in relation to security rules.
- The organizations are accepting accountability for the security policy

Management: In order to develop safeguarding policy and oversee its execution, management is in charge of establishing the department of security.

- Department of Security: The tasks of this division include developing, disseminating, and carrying out the security policy. Educating and training staff members about the procedure is another duty.

-Users: Users must abide through the guidelines provided by security regulations.

-Identifying the enforcement power: A security policy has to have the ability to be enforced in order to be relevant. If not, the policy will remain a printed document. Organizational regulations or laws may be utilized to enforce policies.

D. Risk analysis and security matrix creation

Risk analysis determines the potential hazards associated with assaults on the network, data, and resources of the company. Determining the danger estimations in various network segments and putting in place suitable security measures are the goals. Depending on the significance and potential severity of the danger, three categories can be used: Low Risk, Medium Risk, and High Risk. The users of the system should be identified when the risks have been determined. The different categories of users are as follows (Weiss, 1991; Stallings, 2002; Hamed and Al-Shaer, 2006; Levy et al., 2007; Lelarge and Bolot, 2008): Administrators are internal users in charge of overseeing the resources on the network; Users who are internal and need more access privileges than other users are prioritized; Internal users have general access permissions; Business partners are external users who ought to have access to certain resources; Other: External users or customers.

The combination of networks of computers and the World Wide Web has altered both public and private sector processes, increasing overall effectiveness and productivity. This technology growth has greatly influenced different elements of daily living, changed social behaviour and communicated habits.

Networks of computers and internet access have simplified procedures, allowing for more rapid and effective procedures. In government, internet platforms make it easier to file taxes, renew licenses, and access public information. For the commercial sector, the Internet has transformed the management of supply chains, interaction with consumers, and communication within the organization, resulting in significant efficiency improvements.

E. Implementation of Security Policy

A responsible individual or board establishes the security policy after determining the needs of the firm and conducting a risk analysis. Before the security strategy is put into effect, the following requirements must be fulfilled;

- As the policy is being prepared, participation has to be guaranteed: When drafting the security policy, it is important to make sure that the greatest number of individuals are involved. To develop the regulations, a number of consultations with users should be held. If this isn't feasible, you should at the very least get in touch with the server and module administrators as well as the local system managers.
- The policy should adhere to standards: There are a number of reasons why an organization's security settings might become disjointed and fragmented. These circumstances include spin-offs and mergers. Service delivery to clients, staff, and partner organizations will also be required. It could thus be essential

to draft unique policies for every department. When creating security policies, standards must be followed in order for various security practices and policies to coexist peacefully.

- Another instrument for security evaluation is auditing: It is not, however, continuous as monitoring; rather, it is carried out on a set schedule, according to pre-established standards, and any modifications are recorded.
- The policy ought to be made public and approved by management: Obtaining the management's permission and, if at all feasible, notifying every unit of the security policy via formal letterhead are prerequisites for putting such regulations into effect. The purpose of this letter should be to explain the rationale for the security policy's creation as well as its contents, which should provide access details for more information. It should be mentioned that implementing changes and limitations without administrative backing might lead to a number of issues. Additionally, it must be made sure that users may always view the security policy online.
- The following procedures have to be part of a proper audit: looking at the system status from every perspective. Presentation of every danger that has been recognized. deciding on the inspection's frequency. Monitoring of the applications' adherence to the guidelines.
- Following their creation and announcement, policies ought to be put into effect: The systems or network devices that need to be secured must have the necessary technical settings established in order for the policy's rules to be implemented. Firewalls and access lists, for instance, should be used to build the access rules in the security matrix and determine which servers are accessible through which protocols. Above all, though, security systems need to be regularly evaluated, a risk map created, vulnerabilities found in the system, and appropriate actions implemented. The logs may be examined to see whether the security policy's objectives have been met technologies that provide more thorough information than log reports and list the resources used by whom and for what purposes (Barman, 2001; Stallings, 2002; Hamed and Al-Shaer, 2006; Levy et al., 2007; Lelarge and Bolot, 2008; Cárdenas et al., 2008; Network Security Assessments: Importance and Best Practices, 2024; Network Infrastructure What Is a Network Security Assessment?, 2024).

F. Certification of Safety

Sharing knowledge between domains is typically not secure. The following paper's primary accomplishment may be summed up in two ways. Initially a multi-granularity security controller framework is suggested, including a basic controller component and an individualized multi-granularity safeguarding module. Secondly, the distributed controller is suggested to use an encrypted communication method, and a prototype of this system is put into practice. Specifically, this method can employ the boundary switching as interdomain representatives, in which the controller uses specific packets to convey information to the secure tunnelling. Electronic certificates and inter-domain controllers might provide a two-step verification for the supervisor (Shang et al., 2018).

The step which is completed once the system's efficacy or all of its security measures have been approved is known as certification. Employee education is one of the activities that adds to the success of the system, in addition to the security of the technology utilized. The creation of the security strategy is one of the certification steps. The others are assessment and measurement, evaluation of risks, verification of systems and certification (Barman, 2001; Hamed and Al-Shaer, 2006; Levy et al., 2007, Cárdenas et al., 2008).

G. Analysis of Threat

Multiple resource-consuming computer systems constantly become the focus of security concerns. The potential for system flaws and resources to be abused in order to obtain system access constitutes a danger. The process of security threat analysis starts with locating these resources. This type of evaluation often entails reporting significant events and ongoing system testing. Throughout the analysis, every system used by the business should be taken into account. The following steps are part of the security threat analysis process: Prioritizing previously discovered threats and developing defence systems in accordance with this priority order are important. Accurate documentation of the reasons these resources require protection is required. whatever danger can be presented to whatever resource and by whom should be identified. It is necessary to identify and record vulnerabilities that have already been found. It is necessary to identify the

vulnerabilities in order to provide security services. After each system resource has been assessed independently, the assessments should be combined (Barman, 2001; Hamed and Al-Shaer, 2006; Levy et al., 2007; Cárdenas et al., 2008; Network Security Assessments: Importance and Best Practices, 2024).

Bier et al. (2007) examines a strategic model where an attacker must select a target to assault and a defence must assign defensive resources to a group of places. In an equilibrium, the defender may choose to leave a site undefended in some situations, or they may choose to increase susceptibility at a specific area even when doing so would result in a decreased risk at no cost.

The best resource allocation might be non-monotonic in terms of the attackers outside choice, the defender chooses public defence over secret defence, and she favours centralised (rather than distributed) allocation of resources (Bier et al., 2007).

III. WEAKNESS IDENTIFICATION AND ASSESSMENT

A system flaw that creates circumstances that might result in threats is known as a security vulnerability. These circumstances are brought about by inadequate security protocols and controls. It is not practically possible to identify every flaw in a system in order to guarantee that it is entirely safe. The components of circumstances are presented as below (Stallings, 2002; Hamed and Al-Shaer, 2006; Antsaklis and Baillieul, 2007; Network Infrastructure What Is a Network Security Assessment? 2024);

(i) *Hardware:* Embedded microprograms controlling hardware components can create vulnerability connections even if hardware-induced vulnerabilities are not the primary source of system problems. The high cost of repairs is one of the causes of this. It is quite improbable that the organization employs an experienced individual, even in cases when the cost of repair is little. This individual could be available, but there could be compatibility issues if the component causing the security flaw is replaced. In light of everything mentioned above, fixing hardware vulnerabilities through software support is the better course of action.

(ii) *Software:* It may come in the form of control, application, or system software.

(iii) *People in Systems:* Sharing passwords without additionally malicious intentions and disregard for security protocols might result in vulnerabilities inside the system.

IV. MONITORING AND OVERSEEING SAFETY

Intrusion Detection Systems (IDS) are used to detect and prevent these intrusions. IDSs are hardware or software systems used to monitor and analyse events occurring on a computer system or network and automatically detect signs of security problems. IDSs identify suspicious activity and report it to system administrators so that measures can be taken against potential attacks or security breaches. IDSs are critical to strengthening an organization's security posture and help minimize potential damage by quickly detecting intrusions (Bace and Mell, 2001; Levy et al., 2007; Cárdenas et al., 2008; Böhme and Schwartz, 2010; Amin et al., 2013).

Monitoring and Overseeing Safety consisted of these some vital issues. These are presented as below ((Bace and Mell, 2001; Stallings, 2002; Antsaklis and Baillieul, 2007; Levy et al., 2007; Cárdenas et al., 2008; Böhme and Schwartz, 2010; Amin et al., 2013);

(a) The monitoring step is crucial for ensuring that a system is secure: To do this, a system of control that shows the system's motions and states ought to be put in place. The error reports produced by these surveillance techniques have been taken into consideration when establishing the current security state. Security staff and management employ these controls when considering if additional efforts are necessary to ensure the security of the system. A wide range of instruments are available for use as monitoring instruments.

(b)Instruments for assessing system Performance: Instruments for assessing network security. Tools for keeping an eye on all activity and network performance. DNS and IP status registers that are dynamic. Application status loggers for file sharing. Tools for transferring files

During system monitoring, not all system data is utilised. Examples of criteria that are utilized in a server monitoring system are CPU performance, memory utilization, disc usage, applications, and security.

(c) When analysing the data gathered via imaging, there are many reporting formats available. reporting systems that provide real-time alerts in critical security scenarios. systems that use graphics to measure conditions or output over predetermined periods of time.

(d)An additional instrument for security evaluation is auditing: But unlike monitoring, which is done continuously, this process is done on a set schedule with predefined criteria, and any changes that take place are recorded.

(e) The following procedures need to be followed in a proper audit examining the system's condition from every Perspective: display of every danger that has been found. deciding on the inspection frequency. Monitoring the apps' adherence to the guidelines

Intrusions are usually caused by hackers or unauthorized users gaining access to a system or network. Such intrusions can come from two main sources:

- Internal Threats: When users who already have access to the system abuse their privileges to gain additional privileges or abuse existing privileges. Such threats are usually carried out by employees, contractors, or other authorized users.
- External Threats: Attacks by unauthorized persons or hackers over the Internet. These attacks are usually carried out by malware, viruses, trojans, or other types of attacks that target systems' vulnerabilities.

V. CONCLUSION

Three basic elements of security are addressed by security management of information technology (IT): identification, prevention, and reply. Since each of these elements is essential to the operation of successful security systems, attention should be taken in their development and implementation. But companies have always prioritized prevention over detection and reaction. Ultimately, if dangers are avoided, there is no need for notice or action. Organizations have recently come to the realization that security concerns cannot be completely eliminated. Consequently, detection-based methods have begun to acquire traction in the field of IT security. Cloud hosting suppliers for IT may use guidelines to control their networks similarly to how traditional networks are managed. Internet Service providers may employ policies to set access control limitations for their offerings, while cloud service customers may also state their privacy rules using policy language. Policy methods and associated technologies may be used across several aspects of a cloud infrastructure within IT security management.

The network's ubiquitous impact on both business productivity and personal life demonstrates its revolutionary potential. The Internet remains an influential force in modern life through allowing for speedier interaction facilitating novel approaches to business, and redefining social connections. As technology progresses, its effect is expected to grow, becoming more integrated into the framework of everyday existence and corporate procedures. Networking' infrastructure-free capabilities are spreading over an increasing number of application domains. Security measures regarding attacks in networks ought to be taken into account at every layer due to factors such as random and abrupt users, multiple communications in a susceptible wireless environment, the absence of a centralized management mechanism, and constantly changing network topology. The three primary security mechanisms are the management of keys, intrusion detection, and secure path designation. Security never happens absolutely cheaply. Adding more security measures to an internet connection results in increased computing, communication, and administration complexity. Networks with limited resources must prioritize performance factors, including scalability, availability of services, and security enhancements. Current ideas prioritize cryptographic security, but often neglect network efficiency.

ACKNOWLEDGMENT

I would like to appreciate the executives, the employees of this the organization's plant in this sector, and specialists who gave vital expertise and conversations.

REFERENCES

[1] Amin, S., Schwartz, G. A. and Shankar Sastry, S. (2013). Security of interdependent and identical networked control systems. Automatica, 49(1), 186–192.

[2] Antsaklis, P. and Baillieul, J. (2007). Special issue on technology of networked control systems. Proceedings of the IEEE, 95(1), 5–8.
[3] Bace, R. and Mell. P. (2001). NIST special publication on intrusion detection systems. SP-800-31. National Institute of Standards and Technology.
https://csrc.nist.rip/library/NIST%20SP%20800-031%20Intrusion%20Detection%20Systems%20(IDS),%202001-11.pdf
[4] Barman, S. (2001). Writing Information Security Policies, Sams Publishing, 240 pages.
[5] Bier, V., Oliveros, S. and Samuelson, L. (2007). Choosing what to protect: strategic defensive allocation against an unknown attacker. Journal of Public Economic Theory, 9(4), 563–587.
[6] Böhme, R. and Schwartz, G. A. (2010). Modeling cyber-insurance: towards a unifying framework. In Proc. of the ninth workshop on the economics of information security. WEIS. Cambridge, MA, USA, June.
[7] Cárdenas, A. A., Amin, S. and Sastry, S. S. (2008). Research challenges for the security of control systems. In Proc. of the 3rd USENIX workshop on hot topics in security. HotSec. San Jose, CA, USA.
[8] Fakhravar, D., Khakzad, N., Reniers, G. and Cozzani, V. (2017). Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network. Process Safety and Environmental Protection, 111, 714–725. doi:10.1016/j.psep.2017.08.036
[9] Hamed, H. and Al-Shaer, E. (2006). Taxonomy of conflicts in network security policies. IEEE Communications Magazine, 44(3), 134–141.
[10] Han, W. and Lei, C. (2012). A survey on policy languages in network and security management. Computer Networks, 56(1), 477–489.
[11] Heal, G. and Kunreuther, H. (2003). Interdependent security. Journal of Risk and Uncertainty, 26(2–3), 231–249.
[12] How to Accurately Define the Scope of an Information Security Assessment, 2017 https://kirkpatrickprice.com/webinars/how-to-accurately-define-the-scope-of-an-information-security-assessment/
[13] Lelarge, M. and Bolot, J. (2008). Network externalities and the deployment of security features and protocols in the Internet. SIGMETRICS Performance Evaluation Review, 36(1), 37–48.
[14] Liu, J., Li, Y., Wang, H., Jin, D., Su, L., Zeng, L. and Vasilakos, T. (2016). Leveraging software-defined networking for security policy enforcement. Information Sciences, 327, 288–299. doi:10.1016/j.ins.2015.08.019
[15] Levy, J., Tran, K., Lydon, P., Pollock, J., Parry, D., Weigand, S., Zhong Chen, Z., Ha, H., Gmuender, J. and Massing, M. (2007). Chapter 3 - Creating and Defining a Network Security Policy, Editor(s): Joe Levy, Khai Tran, Patrick Lydon, Jeremy Pollock, Dave Parry, Susan Weigand, Zhong Chen, Hung Ha, John Gmuender, Mike Massing, In SonicWALL Secure Wireless Network Integrated Solutions Guide, Syngress, 55-78, Elsevier Inc.
[16] Network Security Assessments: Importance and Best Practices,2023 https://www.atiba.com/network-security-assessment/ (Access date: 12.04.2024)
[17] Network Infrastructure What Is a Network Security Assessment?, https://kirbtech.com/network-assessments-explained/ (Access date: 15.05.2024)
[18] Shang, F., Li, Y., Fu, Q., Wang, W., Feng, J. and He, L. (2018). Distributed controllers multi-granularity security communication mechanism for software-defined networking. Computers & Electrical Engineering, 66, 388–406.
[19] Stajano, F. and Anderson, R. (1999). The Resurrecting Duckling: Security Issues for Adhoc Wireless Networks, Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, 1-11.
[20] Stallings, W. (2002). Wireless Communications and Networking, Prentice Hall, 598 pages
[21] Weiss, J.D. (1991). A System Security Engineering Process. In Proceedings of the 14th National Computer Security Conference, Washington, DC.
[22] Yang, H., Luo, H.Y, Ye, F., Lu, S W. and Zhang, L. (2004). Security in mobile ad hoc networks: Challenges and solutions, IEEE Wireless Communications. 11 (1), 38-47.
[23] Zhou, L. and Haas, Z. J. (1999). Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security November/December, 24-30.