THE USA JOURNALS
THE AMERICAN JOURNAL OF ENGINEERING AND TECHNOLOGY (ISSN – 2689-0984)
VOLUME 06 ISSUE07

PUBLISHED DATE: - 28-07-2024
DOI: - https://doi.org/10.37547/tajet/Volume06Issue07-09 **PAGE NO.: - 81-93**

RESEARCH ARTICLE **Open Access**

TECHNIQUES TO PROTECT AGAINST CYBER ATTACKS

Vinas Khalid Kadhim
University of Karbala, College of Administration and Economics, Iraq

Abstract
Strong cybersecurity measures are required in this digital era due to the high risk of cyber assaults on people, businesses, and governments. Protecting yourself from cyber threats is the focus of this study, which delves into preventative and reactive measures. To address security weaknesses proactively, it is recommended that advanced encryption technologies and multi-factor authentication (MFA) be implemented and frequent security audits conducted. Implementing intrusion detection and prevention systems (IDPS), real-time monitoring, and quick incident response protocols are all components of reactive methods. In addition, the article delves into how AI and ML improve cyber threat detection and response capabilities by predicting and fighting cyber threats. Users must have cybersecurity education and awareness because user mistakes are still a significant risk. To protect digital assets from the always-changing cyber threat landscape, this paper seeks to offer a broad overview of successful cybersecurity procedures by reviewing existing tactics and emerging developments.

Keywords Cybersecurity, digital era, multi-factor authentication, advanced encryption technologies.

1. INTRODUCTION

The techniques which are described or which are to be followed in an organisation to protect against cyber-attacks are provided in this essay. Security is the primary concern when we perform any operation or activity. The security is breached by a cyber-attack, which is enhancement to technology and the illegal activity done by an unauthorized user. Cybersecurity is obtained from the combat against spyware, malware, rootkits, and key loggers. The concern is to handle or create a mechanism to protect and prevent against cyber threats by the technique. In the essay, it gives a glimpse regarding the technique used to protect against and prevent it in the team of an organisation and the security to be provided to the team.

Various techniques have developed to prevent cyber-attacks against an organisation or in a team. The techniques are divided into the following with the responsibilities and activity performed in tackling cyber threats, which are listed as Security Information and Event Management (SIEM), cryptography, digital signature, Public and Private Key Infrastructures, Secure Socket Layer (SSL), Transport layer Security (TLS), intrusion prevention system (IPS), Security incident and event management (SIEM), Denial of Service (DoS). The approach provides both concepts and technical insight. The approach introduces the need and features for making attacks go away. For creating a mechanism, suitable techniques we prefer to solve the problem. The techniques described are helpful for running any organisation, in case of security, how security will be handled between the team and the end user/organisation. The advancement of the technique will be done on time, and the required can survive.

1.1. Overview of Cyber Attacks

In this day and age, where more and more sensitive information is making its way to various databases,

protecting data from cyber attacks has become a crucial task. Cybersecurity includes various tactics to counter personnel, information, and hardware security, but the best defense is protection against chronic risks. Firewalls, segmentation policies, virtual private networks, and other similar measures are used to protect against such risks. According to the 2021 Verizon Data Breach Investigation report, there have been 5,258 confirmed breaches and 18 organizations affected, with ransomware attacks making up the majority of them. Techniques to prevent such attacks from being successful were introduced by Joseph Stein (2022), "Basic protection against ransomware involves combining regular data backups and on-access antivirus with volume shadow copies. A more systematic defense includes anti-ransomware and anti-ransomware as well as anonymization mechanisms."

In the early 1940s, the year of development, cyber-attacks were rare. However, the spread of the internet to a global network has led to the increased ease of carrying out cyber attacks, to the financial gain of some and international, political, and war-like means to others. This is further exacerbated by future technologies, which will increase the difficulty to defend against such attacks. This has led to the development of a network of defensive tools and deception techniques such as: - Ports: A port can be likened to a router port, a device port, and a switch port in networking. It acts as an interface to establish a connection between an outer and an inner layer from three communication models, OSI and TCP/IP. The port can be logical, which is used by the transport layer (OSI, 4) and TCP layer (TCP/IP), and hardware port on the device. - Firewalls: Firewalls essentially create a physical barrier or means of control between an internet user and a company's local network. Firewalls employ a set of programs to ensure security policies are followed. - Encryption: Because the internet is so exposed to anyone using it, the likelihood of any one party being considered trustworthy is low. Encryption methods rely on public and private key encryptions, ensuring only the two parties involved in a secure transaction can read the data. - Honeypots: Deceive attackers by wasting their time and resources. - Intrusion detection. - Generic internet-like networks using invasive techniques to trap many users until a high-value user is located and can be attacked. - Secure network architectures.

2. UNDERSTANDING CYBER THREATS

Cyber threats are web-based activities mounted by a person or a group of individuals with the intention of damaging any organization's systems or information, including data theft. The most frequent cyber threats that may damage any company are attempts at unauthorized access, tricks of users and employees, traps of users and employees, intrusion of viruses into the network, etc. Cybersecurity plays a very vital role in organizations as a protective measure to guard against cyber threats. Most organizations are unaware of the understanding of cyber threats and the possibility of damage to their web-based systems. This understanding may help organizations apply protective measures to protect themselves.

Several techniques need to be adopted and implemented at various levels to protect one's own identity from unauthorized access. In general, firewalls, strong identity and access management, encryption of sensitive data, and other security systems are considered the last level of protection on the organization's network. While many organizations implement traditional security techniques like firewalls, strong identity management systems, and encryption of sensitive data on web networks, the understanding of types of cyber threats based on attack characteristics and patterns based on the target systems is missing. Cyber threats are very risky and are recognized as people or requests posing as solid students for more details. A security provider is struggling to minimize any exploration of cyber threats in order to develop protective measures against each type of cyber threat. This involves understanding the effects of cyber threats and how to protect an organization from the effects of web threats. The common techniques of operations to avoid these cyber threats are as follows.

2.1. Types of Cyber Attacks

Psychological inconvenience includes any circumstance where a person's data, gadgets, or different items are signed into or taken, or if they can be. Anonymous hacking is when a digital assailant accesses an individual's PC framework without appropriate permission. A theft is the theft or accessing of another person's framework or data without their permission. When a hacker compromises a low-stage gadget under the guise of being someone else, it's referred to as personation. Perpetrators are known to gain unauthorized use by going around security programming and firewalls through an indirect route when reproductions take place. The likelihood of human failure is on the rise. Cybersecurity program units are responsible for verifying the validity of online utilities that do not need human input. In order to download malware onto an organization's assembly line from an unrelated PC, an assailant installs a phishing postal characteristic attachment.

A Trojan horse is a form of malware that attacks a computer system by gaining entry and making changes to conserve and potentially sell it. A back gate is a form of entry within a computer network that can be accessed by cyber-terrorists and then deployed as a robot for a number of malicious applications. When strike command participants conduct harmful code and ploys under the assumption that an unintended exploitation of computer devices has taken place, it's known as entry. At the heart of a distributed denial-of-service (DDoS) attack are minimized and uninstalled websites and services. Attackers make use of Router Ownership Agreements (BGP) to transmit bogus free information across numerous online service carriers in order to turn address space on. The aim here is to guarantee the illegitimate use of opponents' usernames and passwords.

3. RISK ASSESSMENT AND VULNERABILITY MANAGEMENT

For proactive cyber defense, organizations should regularly identify and patch vulnerabilities to reduce the attack surface. Security vulnerabilities are flaws in a program that are open to exploitation. Although privacy is mainly considered during vulnerability disclosure, a risk assessment is necessary in standard risk management procedures for organizations. This risk assessment not only addresses the potential impact of an attack, but also the fact that the organization has a weak link that could be identified and targeted for an attack. Thus, protecting the organization from cyber attacks by identifying vulnerabilities in a timely manner.

Vulnerability management is the process of identifying, categorizing, prioritizing, remediating or mitigating, and reviewing security weaknesses in systems and the software that runs on them. A vulnerability management solution should identify vulnerabilities in your network devices, set pre-determined actions based on criteria such as the severity or location of the problem, let you decide which vulnerabilities to fix and in what order, and offer clear steps to remediate them or recommend alternative ways to mitigate risk. Managing vulnerabilities in this way makes it easier to identify the most important problems and fix them, leading to a better cybersecurity posture.

3.1. Importance of Risk Assessment

An important feature of successful cybersecurity architecture is to conduct assessments fully and continuously because each measure derives from the result of study. Prior to investment of protective measures, it is equally important to inventory what features of architecture cannot be fixed and find ways to mitigate those features if possible, such as through insurance coverage, isolation, or use of other administrative controls. Once the inventory is complete, the next stage is to conduct a risk assessment. The focus of a risk assessment is to uncover "threats, vulnerabilities, likelihoods, impacts, and potential costs" of a cyber-attack.

Once the risk assessment is conducted, it is possible to learn whether current protections are enough or inadequate. If the answer is "inadequate," it shows network security practitioners where to focus their resource expenditures. The risks determined in the assessment identify the "specific risks" an organization currently faces and "categorize the cause and results of a cyber-incident". Having exact information about the condition of network system architecture by conducting a risk assessment can

"focus attention on the real issues needing to be resolved, often making the choice(s) of platforms and solutions self-evident." This can be important to determine the response needed to react to a cyber-attack. By understanding what and where precisely systems are vulnerable, network security practitioners can focus on putting in measures to protect network assets, making sure there are "adequate safeguards" to prevent unauthorized access.

4. NETWORK SECURITY MEASURES

Segmenting the work according to 5 titles (Level 1):

Keeping the Intruders Out of Devices and Systems during Transition. Techniques to Protect Against Cyber Attacks.

3. Network Security Measures

There is not currently any secret weapon that can be used to detect network malware. Rather, good security practice seeks to protect the integrity and confidentiality of data and implementation of network systems and applications. Although network managers often focus on prevention, broadening the focus to include incident detection is actually more useful. Methods often rely on detecting malicious activity as it happens, or detecting erroneous or unauthorized activities afterwards. Techniques include intrusion detection systems, system log monitoring, assessment of financial data to look for irregularities, and techniques that proactively look for signs of malware in the system. While traffic pattern analysis can help spot typical properties of a worm—either during or shortly after an outbreak—it and other passive methods are ineffective because of the ease with which malware can modify and control traffic; for example, "stealth" worms and morphing worms are designed to thwart traffic-based detection.

Once statistical methods identify that some devices are ailing, these detection systems also need to be able to diagnose the extent of a system's impairment so that measures can be taken. IT personnel can remove a weapon from an unprotected host, for example, or reduce the accessibility of that host to inhibit its status as a platform for autonomous replication of the malicious code. Once stealth is bypassed, the quickest methods of protecting hosts involve examining all programs simple and complex to see if a triggering condition is met—that is, if a program is infectious or exhibits other malicious properties. Examples include using formal verification methods to check that all source code follows programming guidelines for eliminating malware and using static program analyzers on binary code. If a worm infection is identified, tools might be deployed in the network to contain its spread.

4.1. Firewalls and Intrusion Detection Systems

A firewall is a combination of hardware and software that prevents unauthorized access to a network through the use of packet filtering and keeps unwelcome data from networked computers.

Firewalls attempt to keep out an unauthorized user who could be outside a company or some other network so that interested users can access the desired information without being denied access. Packet filtering allows or disallows a data packet based upon a predefined set of rules. The rules may be specific to a certain type of application, originating computer address, destination computer address, or other criteria specified in the regularly updated firewall policy. Because the firewall only permits data packets that it has been instructed to let through based upon its policy, packet filtering can be a very effective way of stopping attacks. However, some malicious software can craft its packets so that it looks innocent to the firewall, which makes packet filtering alone not completely effective.

An intrusion detection system (IDS) is a software tool or hardware device that sits in the network. It monitors traffic to and from networked computers, hoping to identify malevolent activities that a firewall could let through. There are two kinds of IDS: host-based and network-based. The former acts as a "watchdog" and detects intrusion attempts through the log files that most operating systems maintain. The latter is a network appliance bolted into the network that analyzes passing traffic in real-time. When network traffic is passing, it is checked against predetermined "signatures".

When a signature "fires", the system sends an alert to a security agent, such as a Security Operations Centre (SOC), for rapid analysis.

5. ENDPOINT SECURITY

One of the primary areas where a company can work to protect against cyber attacks is its endpoints. Endpoints are individual computing devices or endpoints on a network, in contrast to the broader network and systems they access. Because different types of work occur at endpoints, which may be located in a fixed office, at home, or on the go, they are especially vulnerable to cyber threats. Hackers consider these access points up for grabs and are likely to strategize to attack them. Therefore, businesses need to invest in software and tools either to cover or limit the range of attack vectors and to introduce rigidity to the devices and protect them from malicious tactics.

Any company would be better served securing itself by ensuring that their employees are using secure devices and deploying measures to mitigate vulnerabilities on those devices. Some modern measures and tools that can offer companies this kind of endpoint security include end-to-end encryption for secure data and safer remote access and cellular networks. Tools that can further reduce and mitigate those risks include antivirus software, EDR, and MDM solutions that can lock down or lock out hosts to minimize access if a device is compromised. LogicMethod method=Professional Enumeration During a perusal of cyber challenges, endpoint security was presented as a challenge. As a starting point, it is a weak place relative to current technology and solutions in security. Because larger network systems are well-defended, cyber attackers are starting to move to the places where the network's "edges" are, such as endpoints.

5.1. Antivirus and Anti-malware Software

5.1. Antivirus and anti-malware software. One of the primary methods used to protect your endpoints from all types of malicious software is antivirus (AV) and anti-malware software. The software contains several methods to scan for and remove malicious software or software behaving maliciously. This includes signature-based scanning, which looks for patterns that match known malicious software; heuristic-based scanning, which looks for characteristics that are known to excel in the malware; and behavior-based scanning, which is a technique used to catch software that acts similar to malicious applications instead of looking at the code. Each type of protective software will look for different things, so it is sometimes necessary to install both an antivirus and anti-malware solution, though it is recommended to use one solution to reduce costs and simplify administration.

Of course, simply having the software does not protect your endpoint; there are best practices that need to be followed as well. The following information should be considered when deploying antivirus software: First, software will need to be updated regularly, typically once per day through either manual or automatic updates. Since most protective solutions use the cloud to communicate information about new threats and get updates to definitions, constant internet access is generally required. Second, on-demand scanning of the endpoint is recommended to catch malware that has entered the network in case the solution does not use real-time scanning. Periodic scanning is also recommended. Lastly, users can often whitelist or blacklist applications based on what the AV and anti-malware solutions will allow users to do. Certain software may need to be allowed or blocked from being executed for overall security.

6. DATA ENCRYPTION

Data encryption is an essential technique to protect sensitive information from cyber attacks. In essence, only authorized parties can access the information, and the attacker who intercepts the data will be unable to read it. Data encryption includes using a cryptographic key to convert a message which is in plain text into an unreadable format which is called cipher text. This must only be converted into a readable form using the same key as originally used to convert it into a cipher text. In order to successfully implement encryption, two processes must take place: a secure encryption algorithm must be used to convert the original text into an unbreakable code, and a secure encryption key is necessary for the

encryption algorithm to do its job with a matching key to change the unreadable code back into its original form.

Currently, data encryption consists of block-based encryption or stream-based encryption. Block-based encryption is widely accepted as the conventional mode of data encryption, which encrypts an information bit in a block's space (same fixed size) in a memory of a data storage device. Any remaining junk bits are simply ignored. Stream-based encryption performs each bit flow separately and uses NOP-blocks conventionally. A great variety of devices use a range of systems based on data encryption standards in order to perform encryption. In modern applications, such as social media applications, e-commerce, and cloud environment, stream-based encryption will be better than block-based encryption. The time factor will also be another impacting factor. In social media applications, encryption overheads are measured from 10% to approximately 40% for block-based encryption and from 17% to approximately 110% for stream-based encryption. With respect to the cloud environment, encryption overheads are not applicable.

6.1. Symmetric and Asymmetric Encryption

Here we are going to describe various techniques used for protecting against cyber attacks.

6.1. Symmetric and Asymmetric Encryption Encryption is the process of transforming plain text into a cipher form so that only the intended recipient is able to access the original data. To do this, there are two main methods: symmetric and asymmetric. Each of these methods has its own characteristics, uses, and type of provided protection.

Symmetric key encryption, as the name suggests, stands for the usage of one key for both encryption and decryption of a message. Symmetric encryption is used to encrypt the bulk part of the data, like video, image, and email, but it is not suitable for lengthy text messages.

Asymmetric key encryption is a system in which different keys are used to encrypt and decrypt a message. It is also known as public key cryptography. Asymmetric encryption comprises two keys: public key and private key. The public key is used for encryption, but the private key is utilized for decryption. Other users can freely obtain the public key and use it to encrypt messages to send to the owner, while the owner can decrypt these messages with the private key. This is used in digital certificates.

Symmetric key encryption involves the use of one key for both encryption and decryption of a message. Its main drawback is transmitting the secret key from one user to another, which is unsafe. Symmetric encryption is often used in securing data at rest, e.g., full-disk encryption or backup drives.

7. SECURITY AWARENESS TRAINING

Security awareness training is a crucial part of any cybersecurity program. Every organization needs comprehensive and ongoing personnel cybersecurity training. In the end, end-users play a pivotal role in a company's security program and, as a result, the chances for successful cyber threats to the network. Still, users continue to click on links or open attachments. Without adequate cybersecurity training, this trend may worsen. Security awareness must be a priority. The enterprise should have an SOC where it is practicable. Obviously, this human element can be the most hazardous of all the company's aspects. Would you enable an untrained janitor to board your server and mess with wires and settings?

Informing your employees about security dangers is a great place to start. There will always be a discrepancy in the relative security understanding of your workers. It is a major understatement in many situations. It should be mandatory training for all staff. One great, albeit expensive, approach is to use a third party to teach the workers about cybersecurity. Occasionally, enterprises can conduct a human error test. This type of test spends time sending phishing emails manually. Then, a security specialist should click on them. When an employee finally recognizes the message, it is possible to provide feedback and praise. In more advanced techniques, you can allow proactive people to see if they can infiltrate your network through social engineering (for a fee). Many top corporate security professionals have come to

believe that providing excessive access is the top cause of safety problems within a corporation.

7.1. Employee Training Programs

When attacking an organization, social engineers typically look for the weakest link - the people. To mitigate this danger, employee training programs are often implemented. For example, employee security training has become mandatory in many large enterprises. This training can take the form of regular security reminders to keep security awareness top of mind. These brief reminders train employees to avoid falling victim to the tactics social engineers use. Given that phishing attacks are one of the most common attacks on employees, beyond social engineering tactics, training in this area often includes developing phishing awareness. For example, a cybersecurity training program attendees could access on a mobile device. This individualized training includes password security, internet hoaxes, social networking and social engineering, internet security, phishing, and encryption.

Problem 2 addresses the creation and implementation of a password policy, which users must be trained to use. Employees may respond positively to such HR programs and conduct such programs by formulating intelligent and company-appropriate security policies. Techniques for conducting the program can be as varied as the program content. showed that a live performance about password security led to changed behavior. Audience members were asked to complete a password audit and were then "exposed to a live performance that focuses on presenting the results (without using names) and characteristics of the passwords submitted by the students." The authors reported an increased awareness of password policy violations. These training sessions may be viewed as part of a more comprehensive corporate-wide program. In order for employees to grasp the complexities of the threats that face them, other employees, and the organization, it might be advantageous to further explore social engineering, or even more generalized, security, awareness.

8. INCIDENT RESPONSE AND DISASTER RECOVERY

8. Incident response and disaster recovery: Incident response is the structured approach to addressing and managing the aftermath of a security breach or cyber-attack. Cybersecurity incident response plans are required to be created in advance to outline the proper and orchestrated response to a variety of cyber incidents. They are designed to help speed up the response time and minimize damage and embarrassment, but also reinforce the resilience of the organization from future threats. Components of incident response include an incident readiness and preparation phase, incident detection and analysis phase, incident containment, eradication and recovery phase, and incident post-activity and continuous improvement phase.

Disaster recovery should also be addressed in official cybersecurity policy, from understanding how employees will know there is a DRP to involvement in strategizing, testing and continuous assessment. The objective is to recover and reestablish normal operations quickly and effectively from any type of disruption.

Authority of recovery plans or systems to recover from an event depends on having reviewed and updated by everyone who is responsible for its elements. Only a regularly assessed disaster recovery plan can assure that your business can resume in compliance with governmental and policy entities with acceptable risk. The DRP must be capable of implementation smoothly with testing procedures, schedules or frequencies must be clear. Assurance is crucial: this ensures the value of the care and stimulates confidence from stakeholders. Documentation should be filed and clear so it may serve as a disposition index for a variety of recovery processes inside and beyond IT. All relevant staff and firms, as required, must be eligible to get it.

8.1. Creating an Incident Response Plan

Planning for the worst can help you be at your best when it comes to detecting and responding to a cyber incident. That's why the first step towards mitigating the impact of a cyber incident is to lay the groundwork by creating a comprehensive incident response plan. The NIST Computer Security Incident Handling Guide provides an

excellent framework for creating an incident response plan. It covers the entire lifecycle of a cyber incident, including identification, handling, and learning from a breach. Six phases highlight the commitment to continuous improvement. The life cycle consists of the preparation, incident detection and preliminary response, analysis, containment, eradication and recovery, and post-incident activities.

Identifying your plans and placements is the center of gravity of incident management. Identify hardware and software assets, how they are integrated, and assess the security options available. For this level of detail, people often turn to your organization's enterprise architecture documentation. Identify requirements for issues of inconsistent security solutions and compliance approvals, protective monitoring, dealing with false alarms, and how to minimize the risk of impact, evidence preservation, and other legal considerations. Carrying out adequate IPC arrangements requires the development of a strategy and effective ongoing governance. Taken together, IPC arrangements, system security, and information security management are the foundations of a risk management plan and can be considered in conjunction with each other. Compliance checking provides evidence of performance and risk measurement to ensure that your arrangements are effective. Compliance gets affected by your efficacy for risk management, your requirements, and what rules and guidance apply to you.

9. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Just because a car comes with an alarm system does not mean it is secured. The same can be said about cybersecurity as simply possessing a business security system - a "one and done" proposition - does not suffice. While a security system may indeed protect explanations from break-ins, exposing system logs in the cloud may not suffice in cybersecurity risk management. Luckily, larger firms also use more advanced systems for tracking these activities; those systems, known as Security Information and Event Management (SIEM) solutions, perform three functions: collecting security data from logs in networks, analyzing system data, and responding to policy breaches.

SIEM systems are critical in aiding a business to respond to anything that affects the system in real time, in order to predict and protect against vulnerabilities, threats, and attacks in a timely manner. In reasonable context, doing so will minimize how much pain firms could suffer as a result of a cyber-attack. In an era of reliance on digital business transactions and technological immersion, data-protection techniques are growing more salient in safeguarding corporate networks.

9.1. Role of SIEM in Cybersecurity

SIEM solutions are a necessity when discussing the combat against evolving cyber threats. Although not easy to detect, SIEM can provide some assurance to the security staff in specific situations. Due to its real-time monitoring, organizations can detect unwarranted activities creeping through the systems. It provides an address in curbing cyber threats into the enterprise's mainframes and software-related assets. To increase the level of credit trusts, SIEM solutions usually come equipped with threat intelligence aspects.

Organizations can use SIEM to get detailed threat assessments from one or more threat intelligence feeds, with some SIEM platform in the form of add-ons or it may be a part of the solution itself. Some solutions will give a quantities amount of information in reference to potential threat actors such as, but are not limited to, their identifying information, what areas they are operating in, what other groups have also confirmed them as a threat group, and what are current vulnerabilities. Threat Intel is a set of information used to help an organization anticipate, prevent, and respond to cyber threats. Threat intel services should be used to shore up SIEM services when managed internally. Organizations are paying a premium to acquire information on what vulnerabilities are found in the wild and how adversaries operate. SIEM is also necessary when meeting regulatory compliance as it collects logs from devices within the network. Having a SIEM solution allows businesses to monitor data regulations, as such business must provide a secure connection to

houses and secure data within its boundaries.

10. CLOUD SECURITY BEST PRACTICES

Cloud computing allows businesses to store and access data and applications over the internet rather than in a physical location like an office building. Leveraging cloud services in the enterprise enables users to work from any location with internet access. Adopting them can boost performance and improve cost-effectiveness by replacing traditional on-site hardware or software.

The shared responsibility model assigns a range of tasks to cloud service providers (CSPs) and cloud users. It maps out where CSPs' responsibility ends and minor aspects of security are left to the user. This model helps in the prevention of data breaches. Although CSPs provide overall security, they have no control over the users' activities. The shared responsibility model is mandatory for the protection of organizations against cyber threats. Therefore, companies must adopt these best practices to act against all possible security risks unique to cloud environments. Here are the strategies to ensure the security inside cloud computing.

1. Determine your level of responsibility. 2. Use multi-factor authentication (MFA). 3. Manage access and permissions. 4. Monitor for change activities. 5. Implement security groups and network access control lists.

10.1. Shared Responsibility Model

While securing cloud resources, one thing important to understand is that customers are also responsible. This is the AWS shared responsibility model for security. AWS is also not responsible for many things. Customers need to understand whether they are responsible for these things, or whether their cloud service provider is responsible for them. Once responsibilities are established, you can go on to implement security. For example, it is the customer's responsibility to protect their content, regardless of the form it is in. In security terms, this is known as determining security postures. Before doing this, though, an understanding of compliance is important. In fact, security is measured through compliance. Security ensures that something is kept safe, providing dependability. Compliance measures the extent to which dependability is aligned with standard guidelines.

A security posture encompasses the policy (the high-level rules), which in turn leads to the implementation of procedures, guidelines, and some automated settings. The deployment of these procedures typically contains operational data, or metadata. The proprietary data or business data is kept on Amazon S3. The user client may have proprietary sensitive or personal data on their own physical computer, OWASP Top 10 attacks ignore such physical computers. Cloud computing security is breached through attacks on the cloud, for instance through the server, hypervisor or physical infrastructure. The local app actually has the OWASP Top 10, because it interacts with resources let in from the cloud, such as web pages, services, and so on. Also, security for the AWS parts deployed on customer premises is not considered.

11. MOBILE DEVICE SECURITY

Securing a mobile device is a colossal challenge with so many threats that target the device's operating system, management systems, and applications. These threats also target its communications systems and control the Wi-Fi and Bluetooth connections. Such systems are meant to serve the user and support them with their services, while being localized at places such as stations, commercial stores, gas stations, etc. These systems are controlled remotely by the user's applications.

Protecting mobile devices requires specialized mobile device management, hired by the administrator or owner of the device. This includes keeping the operating system and embedded hardware updated, banning connections in the event of danger, and protecting system services and calling interfaces. It is important to note that securing the system should also prevent impairing its numerous calls.

Modern device security is mainly based on the deployment of secure apps, even though malware can still operate if the operating system itself is clean.

Mobile apps generally require concise network call

features, as well as geographic location and connectivity services. However, these features can lead to serious security problems. Applications may behave maliciously by using trusted debuggers and bypassing built-in protections. Network behavior analysis, application stores, and the many software-quality improvement tools available offer poor managing protection. This is due to their need for a large labor force, software company approval, and advertising pop-ups on devices that may annoy users.

It is difficult to deploy reliable approaches for mobile devices because networks change from place A to place B.

11.1. Mobile Device Management

11.2.13.3.1 Mobile Device Management

This practice and tools encompass mobile device management (MDM) - functions commonly required, given the fact that smart, connected mobile devices increasingly dominate modern businesses. MDM is the process of centrally administering, protecting, and preserving mobile devices all across any of an organization's various locations.

There are many assumptions or issues about protecting an organization's wireless infrastructure which may or may not be valid. Vendors help perpetuate some incorrect notions, while information security firms sometimes overblow mobile-device vulnerabilities. Assumptions include: - Everything will connect wirelessly. - Everything that wirelessly connects to something else is inherently insecure. This is not exactly true. This assumption can be validated via transmissions between a laptop and fixed base station. - Any unauthorized transmissions discovered by the client card type are dangerous rogue connections. - Wireless equipment is inherently hard to manage and protect. Vendors who say so, however, come to sell complicated multi-tiered security solutions.

Assumptions like the above are generalizations based on a scared or optimistic perception of the technology. MDM refers to the set of people and tools that also manage the mobile devices people use for work. While communication with a central management server is crucial, the management components (control functions) - that is, physically available equipment and substantive processes and tools - typically encompass these types:

- Registration: Register a device to get it manageable. - Policy enforcement: Make sure that wireless devices adhere to appropriate network policies. The network can also verify which devices are trying to attach and inform the network operations team to assist vulnerability assessments. - Remote device management: Typically, involve setting up management and support tools for users or for network operators to provide patches, configurations, voice-mail messages, software updates, passwords, and security settings and reconfiguring the client. Because management from all of one equipment vendor is a rare scenario, these capabilities can be collapsed to one enterprise management technique. - Platform independence or platform diversity: Operational overhead for the enterprise depends on software and management tools being available in all networking equipment and encompassing all types of client software and hardware in use. An enterprise may need to have different techniques for different generations of client hardware, for example, wireless LAN cards, short-range RF data cards, and different kinds of WAN data cards. Different OSs and their differing capabilities are in play. Higher-end devices such as PDAs can also let a user perform functions that the user's notebook cannot. Wireless service providers also require that, in general, the provided security techniques not completely protect all devices. If it did, the service would have difficulty breaking into the market. Management capabilities for enterprise/secure wireless networking and related virus protection, network site survey, and device and configuration-resistance scanning are provided.

12. PHYSICAL SECURITY MEASURES

12.1 Overview Physical security comprises the various physical measures that are used to control and monitor access to an organization's IT infrastructure and the various facilities that house the IT facilities and the critical data. Typically, an organization will have several tiers of control over

the area they choose to house their physical IT resources. A few organizations may even use offsite data centers or facilities managed by managed services providers or cloud service providers. In comparison to this, most organizations will own and manage their own computer centers and office buildings for in-house storage. There will be universal readers and card access systems to monitor and limit access to sensitive areas.

12.2 Personnel Security Awareness and Training The concept of personnel security and awareness is a system in which human physical and system assets maintain their protection. Personnel in an organization are under the influence of training under security perspectives to enhance their awareness. Several organizations are implementing related methods to produce a security organization. There are several methods used such as awareness week, monthly training, regular information security activities, and others. They have also integrated threats, security threats, physical threats, and other forms of safety threats into a single framework. Physical security, information security, human resource security, onetime security, access control, and personnel training are also concerned. Therefore, personnel are a standout point in the system because they are the potential victims of social engineering attacks, and linking up these two functions must involve the personnel in physical security, information security, etc. The security awareness and training establish a security element in the IT infrastructure development. Some organizations don't implement ISSA or the CISSP standard requirement because of their false confidence in technology and the protection they already have in place.

12.1. Access Control Systems

Despite the most accommodating security protocols, technologies, and training, a determined aggressor can often gain the trust of an insider and make it possible for them to gain physical access to an EOP.

Access control systems consist of technologies and procedures for denying access to unauthorized personnel (deterrent) or detecting unauthorized personnel attempts (detection) to gain entrance into a potentially sensitive area. There are a number of physical access control systems in use as of this e-book's publication. The most frequent of these is the lock and key, which still provides the lowest level of protection. More secure are electronic access control systems which range from simple keypad readers to complex biometric (e.g., fingerprint readers) identification systems. It is important to note that although these systems incorporate some of the same sensors as other IDS technologies, they are normally treated as a part of physical security rather than as a fortification against external cyber threats. Access control systems on or integrated with the EOP and critical networked systems, however, can provide another layer of defensive action. Additionally, proximity cards, key reader locks, and/or biometrics might be used. Regularly modifying entry codes/cards for authorized personnel might also add to the layers of security already present.

13. REGULATORY COMPLIANCE AND STANDARDS

It is legally obligatory for companies to comply with regulations and standards. The financial consequences may be significant for failing to do so. Legal requirements include minimum legal standards of cybersecurity and crucial safety mechanisms. Various standards are used by companies across various industries, such as ISO 27001, NIST SP 800-53, CIS Controls, and CIS Benchmarks, to control and enforce specific compliance requirements. In the area of finance, other sectors deal with money, such as healthcare, and financial instruments are discussed in detail.

European Union regulations, including the General Data Protection Regulation (GDPR), are covered. Part of European Union regulations. Since May 2018, GDPR has influenced cybersecurity dramatically. The secure processing of confidential data of partners and customers is key to company cybersecurity. Other local laws of countries have implemented GDPR standards. HIPAA, the US Healthcare Insurance Portability and Accountability Act, is important. It covers security issues related to private and shared healthcare data. It forces healthcare companies to use algorithms, breaking them into the following subsets: 7.1 organizational, 7.2 human, and 7.3

technological. And healthcare experts say other companies interested in general cybersecurity staff can extend the application of research in teaching systems, much of which is medical.

13.1. GDPR and HIPAA Compliance

In the modern setting, organisations worldwide are subject to increasingly stringent data protection laws, one of the more prominent of which is the General Data Protection Regulation which came into effect in 2018. Companies in the United States are also subject to the Health Insurance Portability and Accountability Act (HIPAA), which establishes data protection requirements for numerous data types in the health sector. Achieving compliance with HIPAA or GDPR involves showing proof of robust data protection practices, with information security management, data loss prevention tactics, and secure data access controls being vital. Organisations looking to avoid potentially significant compliance failure fees, therefore, have a vested interest in defending their systems against cyber-attacks.

One element of GDPR in particular that bears relevance to cybersecurity practice, and is applicable when it comes to news reporting, is the explicit requirement for businesses to protect the confidentiality and integrity of their IT systems. As attacks against healthcare providers become more numerous, the GDPR compliance status is under scrutiny. In this section, several individual steps are provided with a view towards a cybersecurity manager who may be looking to protect digital healthcare systems.

A legal requirement, both HIPAA and GDPR require that organisations have at least a basic level of cybersecurity practices in place, and that more stringent standards are implemented in relation to sensitive data. Numerous investigators and legal or data security agencies have been recommending crucial actions and validating their effectiveness. It is unclear, however, whether the proper implementation of these measures is being enforced in some businesses, leading to significant rates of cyber and ransomware attacks in addition to supply chain information security risks. In the Deposit Library of the STACC Research Center, for this dataset, we believe that increased confidence in cybersecurity measures may prevent or hinder the detrimental impact of data safety events.

14. EMERGING TECHNOLOGIES IN CYBERSECURITY

The accelerating timeline of novel and disruptive technologies that have implications for our collective security is challenging the policy and governance systems in place today. Strategic cyber research looks at the policy and governance implications of cyber operations and strategies. However, cyber intrusion research details scenarios, observations, and analyses of general policy and governance challenges. A broader research agenda examines the impacts of rapidly emerging technologies on military operations and relationships. In some cases, these applications are not widely recognized as having military relevance that could impact military activities such as operations, force planning, and research, or foreign relationships and threat perceptions.

AI has captured imaginations and spurred investments. In cybersecurity, AI- and machine learning (ML)-driven applications are increasingly seen as a cybersecurity imperative and an opportunity to tip the scales back against opponents. Despite all the storylines, real-world evidence conflicts about the current state of AI-driven cybersecurity as opponents more rapidly than defenders leverage AI within their operations. As headquarters pursue AI and machine learning investments and proof of concepts, a more substantive investment area will be in data collection and preparation, often outsourced to consultants or firms familiar with their cybersecurity challenges. The military's move into the cloud also generates the type of data volume and access AI and machine learning technologies seek. Plus, with industry solutions claiming to optimize costs and shifts in defense policy that emphasize operational challenges over acquisition hurdles, purchasing AI and machine learning capable tools, expertise, and assessments is now feasible.

14.1. Artificial Intelligence and Machine Learning

Artificial intelligence has widespread implications

for intrusion detection and log analysis in the context of machine learning. A clear technical, yet often interesting, survey of machine learning for intrusion detection and log file analysis, as well as a more recent attempt to engage network behavior analysis, reveals that machine learning could be put to numerous and complex approaches for cybersecurity purposes. Techniques that automatically process large datasets, derive models of "acceptable" and "suspicious" activity, and also detect network intrusions function in this context. Good reviews or more specific in the context of network security are also available from machine learning techniques.

While some of the illustrative machine learning techniques are essential for such use, many others could be traded or modified to perform pattern detection and unsupervised learning, from clustering to artificial neural networks or genetic algorithms. Possessing technical aspects, alternative detection of anomalies provides automatic analysis and response to threats and potential intrusions. Machine learning also extends to automated threat response, which will take action to mitigate threats or intrusion detection from an attacker, using a bounded model of an intrusion detection system that employs techniques from AI.

15. REFERENCES

1. Abou-Assaleh, T. and Chuluundorj, E. (2010) Cyber-Physical Attack Threats, IAS-2008-41-L. Carleton University National Capital Institute of Telecommunications.
2. Alves, T. et al. (2010). Cyber Range: Challenges and trends. J. Def. Model. Simul. 11, (1): 17-83.
3. Gerndt, M. (2015). Defining cyber defense exercising. In Proceedings of the 3rd International Conference: Future - Security, Bonn, Germany, 16-17 September 2015. pp. 9-16
4. Park, Y. and Sandri, S. (2003). Potential game hazards and cost of anarchy in malicious environments. In The Sixth International Workshop on Discrete Event Systems, 2003. Proceedings. In this Issue, 13-15 October 2003,
5. Hubei, China Lublin, A. (2016) Ships in Pompeii. How to Train Cyber Security Experts. In@risk - Journal of Risk Analysis, Vol. 4, No. 12, p. 6-11. Available online:
6. Zørnemann, T. F. (2001). Test management for distributed real-time systems. University of Warwick.
7. Lublin, A. (2012) Energy Supplies: A Bird's Eye View of Modern Europe. Special Editor T. Boettger. In: NATO Operations in an Immutable World - Defence against Terrorism. Special edition for the conference "Security and Defence Explorations of Change", Vol. 39, ISSN 1864-6619, September, 2012.
8. Wedde, L.F. (2008). Applications from the art and theory of games - a classifying survey. In Paul W. Goldberg, Norman Y. Foo, Mark Thorwart Goldszmidt, and Lewis Girod, Editors, First international workshop on games and emergent behavior (2005). Games for multi-agent systems, pages 212-225, Berlin, Heidelberg. Springer-Verlag.