The Importance of Implementing Security Management in the Era of Digital Transformation

Achmad Fauzi[1] , Ratilla Amanda Edwar[2] , Teti Aliyanti[3] , Ayu Nur Jannah Milawati Candra[4] , Amelia Seli Febrianti[5] , Iqbal Al Baihaqi[6] , Aditya Aji Nugroho[7]

[1,2,3,4,5,6,7] Universitas Bhayangkara Jakarta Raya
achmad.fauzi@dsn.ubharajaya.ac.id[1] , ratillamndaa@gmail.com[2] , tetiiiiialynti@gmail.com[3] , nurjannahayu781@gmail.com[4] , ameliaselif@gmail.com[5] , iqbalalhq090@gmail.com[6] , adityaajinugroho10@gmail.com[7]

*coresponden author

ARTICLE INFO

Keywords: Cyber Security, DDoS, Malware , Implementation

Received : 04, June
Revised : 12, June
Accepted : 19, June

ABSTRACT

Cyber security is an important aspect of the increasingly complex cyber threats. This research uses a qualitative approach, namely a method using a literature review. This study was conducted to examine how events implement security management in this developing era and how to maintain data security. Human Resource Security is also very important in facing various threats in the digital transformation era which include SQL Injection, Phishing Attack, Fake News, Denial of Service, Malware & Ransomware, and others. Hackers' motivations for launching malware and DDoS attacks are usually to gain access to sensitive data, disrupt business operations, or exploit systems for illicit purposes. The goal is to consume system resources and cause business system failure.

INTRODUCTION

In the era of digitalization, technology plays an important role in life in various aspects of globalization which is developing with the internet which provides information easily and quickly in order to survive in today's artificial intelligence competition. Currently, the concept of cyber security must be interpreted as one of the country's territories that must be protected as a state obligation to secure its borders. Now, interactions between international relations actors are not only carried out on land, sea and land. Interaction between actors is also carried out in virtual space to achieve other options in achieving state interests.(Triwahyuni & Wulandari, 2016)

The formulation of cyber security policies is an important aspect in responding to increasingly complex cyber threats. One of the main focus areas is technology development, increasing public awareness, and developing collaboration between government, the private sector, and society with the aim of improving cyber security. It is important to increase public awareness of the nature of cyber threats and develop strategies to improve cyber security. The strategy must include the implementation of strict regulations, the establishment of the National Cyber and Crypto Agency (BSSN), and the development of innovative cybersecurity technology.(kita, 2024)

In order to improve cyber security, implementing a risk management framework is very important in dealing with increasingly complex cyber threats. These strategies involve various aspects, including technological development, increasing public awareness, and cooperation between government, the private sector and society. (HRF, 2022). Disaster recovery contingency implementation planning must involve the use of an emergency response team that has been trained to respond to cyber attacks from members who have special skills and knowledge in cyber security who will then be responsible for identifying and monitoring attacks, as well as taking the necessary actions to reduce losses and restore the system.(Purbo, 2023)

Implementing technology and security management solutions is critical to protecting countries and organizations from cyber threats and ensuring data security. As has been implemented in Indonesia, which is responsible for monitoring and regulating cyber security in this country, as well as assisting other countries in dealing with cyber threats, namely the Cybersecurity and Information Systems Agency (CISA). Apart from that, in Singapore there is a Cybersecurity and Data Protection Act (CDPA) which can update cyber and data security laws, as well as strengthen the government's role in supervising and regulating cyber security in the country. Here are some examples of cyber security for smart devices that need to be used, such as: Firewalls are used to prevent unauthorized access to systems or networks. Intrusion Detection System (IDS) software is used to detect and stop cyber attacks. Secure Sockets Layer (SSL) is used to protect data sent over the internet. Virtual Private Network (VPN) is used to protect data sent over the internet, especially when connected via public Wi-Fi services.(Adhiaksa, 2021)

After securing the data, it is best to maintain confidentiality and avoid hacker attacks, we can use key management. Automated key management is a system designed to facilitate more effective and efficient key management at a business location. The system uses radio frequency identification (RFID) technology to identify locks and monitor unlocking, the time of the event, and the specific key used. The system also features high-level security and management access control to all keys, allowing monitoring of who opened the cupboard, when, and which keys were taken. Additionally, it ensures that every key is returned to the cabinet on time.

The causes of data leaks can be related to several main factors: Human activity and computer systems. Human error is one of the factors of error caused by human activities, factors such as inadequate training, ignorance, poor decision making, technical errors, and policy-based errors contribute to vulnerabilities in information security. Task interruptions and switching between subtasks can disrupt the flow of work, causing action slippages that compromise the handling of sensitive data. . Another factor is the computer system, such as programs specifically designed to damage computer systems and enable theft of company information or what is usually called Malware. (Utama, 2023).

Digital transformation is closely related to smart manufacturing and the Internet of Things (IoT) as well as Big Data and AI. In facing the challenges of digital transformation, organizations must be able to ensure that digital transformation does not only focus on technology strategy, but also on developing human resources within the organization. Human Resource Security is very important in facing various threats in the digital transformation era which include SQL Injection, Phishing Attack, Fake News, Denial of Service, Malware & Ransomware, and others. (Munandar, 2023). It is necessary to increase employee training and awareness in an effort to improve the implementation of cyber security in an organization. For example, holding cyber security training is very important to improve the quality of human resources in the field of cyber security. This activity evaluates the impact of cyber security training on increasing knowledge, skills and awareness of cyber security risks.

A number of activities can be carried out to increase employee awareness of the vulnerabilities inherent in human resources in maintaining cyber security. One of these activities is Cyber Security Training. Cyber security training should start with efforts to increase employee awareness of existing cyber threats. It is critical for employees to be able to differentiate between different types of cyber attacks, understand how to report any attacks they encounter on company systems, and have the courage to report lost devices, phishing attempts, or similar incidents to the appropriate departments. within the company. Additionally, it is very important to cultivate cyber security skills among employees to protect the company from cyber attacks. When employee awareness is increased, security practices are taught, and necessary cybersecurity tools are provided, companies can reduce the risks they face and ensure the security of their valuable information.

Following training to increase employee awareness, identity management is critical for organizations that want to improve data security and privacy, as well as improve the quality of service and relationships with customers. Such as increasing data privacy and security, as well as optimizing identity and access programs.

The phenomenon that occurs in Cyber attacks on healthcare systems involves data theft through malware, hacking, and DDoS attacks, posing a threat to the security of patient data and system functionality that occurs during the Covid-19 pandemic. (Jasmina M. Veličković, 2023). According to research from (Evans, Maglaras, He, & Janicke, 2016)shows that 80-90% of security breaches in the United States and the United Kingdom are caused by human error. These two countries account for more than 90% of reported data breaches. Additionally, IoT issues in home automation devices can trigger data security issues such as personal data exploitation, unauthorized device control, and network access violations as more and more devices are connected to the internet.(Solorzano, Gutiérrez, & Gordillo, 2023)

From the problem above, the problem formulation can be made as follows:

1. What reasons drive hackers to launch *malware* and DDoS attacks, and what is the best way to identify, prevent, and respond to these attacks effectively?
2. What is the impact of not training employees on cybersecurity regarding *phishing* and *spear phishing attacks* ?
3. How to manage security risks associated with software and firmware updates on *Internet of Things* (IoT) devices distributed across a network?

LITERATURE REVIEW

Implementation of security management

With security management, we can organize or plan security so that this can be avoided. Security Management is a system that provides a comprehensive and integrated understanding of the planning and design of appropriate, effective and efficient security systems, in accordance with special circumstances and conditions that may arise, especially in the context of potential threats or disturbances. This is also useful for preventing losses for the company as early as possible (Loss Prevention). (Rayhan, Alfaridzi, Saputra, & Sinlae, 2023)

Security management implementation is the process of implementing strategies, policies and procedures to protect information assets and systems from threats, attacks or security breaches. This involves identifying risks, developing security controls, implementing preventive measures, detecting, and responding to security incidents.

the process of implementing the security controls that an organization has established to protect their information assets and systems from threats, attacks, or security breaches. This involves concrete steps such as developing security policies, implementing technical and administrative security controls, implementing security training for employees, and continuous monitoring and evaluation to ensure security effectiveness. Implementing security management allows organizations to manage security risks well and maintain the continuity of their operations in an era full of digital security threats.

Digital Technology Transformation

Digital technologies are changing the way businesses, governments and societies use digital tools to transform their processes, products, services and business models. It involves using information and communications technology (ICT) to create new value, increase efficiency, and create better user experiences.

Some of the key trends in digital technology transformation include:

1. Internet of Things (IoT): IoT allows physical objects to connect and exchange data over the internet. This allows us to collect more data, monitor things in real-time, and automate processes.
2. Artificial Intelligence (AI) and Machine Learning: AI and machine learning enable systems to learn from data, identify patterns, and make decisions without human intervention. They are used in a variety of applications, from data analysis to intelligent decision making.
3. Big Data: Big data is a term used to describe large amounts of data that is managed and analyzed to identify trends, patterns, and insights that can be used for decision making.
4. Blockchain: Blockchain is a technology that enables secure and transparent digital transactions without the need for a third party. It is used in a variety of applications, including finance, supply chains, and digital identity.

The transformation of digital technology has changed the way we work, interact and live daily. As technology changes, it is important for companies and individuals to keep up with the latest trends to stay relevant and competitive. The phenomenon of digital transformation has become a widespread phenomenon and has far-reaching impacts and impacts on various sectors of life, bringing significant and broad impacts and influencing the direction of development. (Ikhsan, 2023)

Is the process by which organizations use digital technology to change the way they operate, interact with customers, and create new value. This involves the adoption of technologies such as cloud computing, data analytics, artificial intelligence, Internet of Things (IoT), cloud computing, big data, and process automation to increase efficiency, innovation, and competitiveness.

The process by which organizations change the way they operate, interact with customers, and create new value by leveraging digital technologies. Digital transformation not only involves the use of new technologies, but also affects the culture, business processes, and operational model of the organization as a whole. The goal is to create a better customer experience, increase productivity, and create new opportunities for growth and development.). Digital transformation can be defined as the modification (or adaptation) of business models, resulting from the dynamic pace of technological progress and innovation that triggers changes in consumer and social behavior.(Tulungen, Saerang, & Maramis, 2022)

Human Resources Security Management

HR (human resources) security management is an approach used by organizations to safeguard confidential information, sensitive data, and intellectual assets from internal and external threats. This involves implementing policies, procedures and practices designed to ensure that HR personnel who have access to sensitive information are adequately protected.

Some important HR security management practices include:

1. Careful Recruitment and Selection: Ensures that prospective employees are rigorously tested to ensure a high level of trust and integrity. Additionally, background and reference checks are conducted to ensure the correctness of the information provided by prospective employees.
2. Security Training and Awareness: Employees are provided regular training regarding information security practices, company policies, and appropriate actions to take in the event of a security threat. High security awareness among employees can help prevent security incidents. This is achieved through assigning access rights, implementing double authentication, and observing user activity.
3. Security Policy: Develop security policies that are transparent and consistently applied across the organization. This policy should cover device utilization, network access, password management, and other security measures.

HR security management is an important component of an organization's information security strategy. By implementing these practices, organizations can mitigate security risks and protect their sensitive information from existing and potential threats. Information security is an important aspect in human resource management, especially considering the increasingly sophisticated information technology. The goal of information security is to prevent threats to systems and to detect and anticipate potential threats. (Oktafiani, 2020)

METHODOLOGY

This research uses a qualitative approach, namely a method using *a literature review* . This study was conducted to examine how events implement security management in this developing era and how to maintain data security. The data was compiled from various relevant previous journals and articles relevant to the problem raised.

Table 1: Previous relevant research results

Title & Author	Research Results	Research Equation	Research Differences
Cyber security analysis in the digital era "security challenges and strategies" (Muslim, Amanda Sephira, Muhammad Hanif Abrar, Semmy Loreno Suranta Warning the Wind, Habiebie Hidayatullah, 2024)	The main challenges that organizations face in ensuring the security of their IT systems and presents effective security strategies to overcome these challenges. Threats such as malware attacks, phishing and insider threats are becoming increasingly complex and often require a comprehensive approach. Important strategies to implement in this context are data encryption, real-time security monitoring, and employee training on security.	Both articles discuss data theft through malware, phishing attacks, and DDoS attacks	The previous article focused more on in-depth analysis of the cyber security challenges faced and formulating effective security strategies , while this article focuses more on implementing security strategies in facing technological change and digital transformation.
Influence analysis needs training culture security cyber as	Considering that technology and knowledge about hacking efforts in cyber crime are developing very	Both articles discuss human resource security	The previous article explained security training among state

Attempt development of competency for civil state apparatus in the digital (Sri Light Khoironi, 2020)	quickly, it is necessary to anticipate investment in human resources through cyber security culture training.		civil servants in the digital environment, while this article explains more specifically Human Resources security training
Privacy and Security Application IoT In Life Everyday Challenges and Implications (Fauzan Prasetyo Eka Putra, Selly Mellyana Dewi , Maugfiroh , Amir Hamza [1] , 2023)	The Internet of Things (IoT) has a major impact on product quality and product distribution monitoring. As defined by Fawzi Behmann, the term "Internet of Things" (IoT) refers to using the internet on a larger scale, enabling computing and mobile connectivity, and then integrating these technologies into everyday activities. The Internet of Things (IoT) has provided many benefits in human activities in daily life. The development is rapid, and will continue to develop in the future. However, its application in today's society also raises challenges and implications related to security and privacy.	Both articles discuss firmware updates as well as software tools	Previous journals emphasized security and privacy challenges related to the use of the Internet of Things (IoT) in the context of everyday life, while this article discusses the Internet of Things (IoT) in facing the challenges of digital transformation.
Web Server Defense Method Against Distributed Slow HTTP DoS Attack (Molavi Arman, 2020)	Slow HTTP DoS attacks are one of the DoS attack methods that target HTTP servers. This method hampers the service by flooding it, creating a collection of connections with slow and large requests to the web server. It is known that slow HTTP DoS attacks by a single attacker can be effectively prevented by limiting the number of connections for each IP address. The threat of DDoS attacks is increasingly serious, so it requires effective defense methods against distributed slow HTTP DoS attacks.	Both articles discuss preventing DDoS attacks	The previous article explained more specifically, while this article discusses it in general terms only
Urgency Regulation Special and Utilization Artificial Intelligence in Make Protection of Data Personal in Indonesia (Day Sutra Embedded , 2021)	Maximum data protection for personal data security. With the presence of Artificial Intelligence, which is more effective and efficient, it is able to prevent system errors and minimize the risk of personal data leakage due to human error.	Both articles discuss data leaks due to human error	The previous article used the normative juridical method, while this article uses the *literature review method*
Deepdefens: A comprehensive framework for DDoS Attack detection and prevention in computing. (Mohammed OuhssiniA, Karim AfdelA, Elhafed AgherrabiB, Mohamed AkouharC, Abdallah AbardaD, 2024)	Aladaileh et al. (2023) performed an entropy-based approach to detect low- and high-level DDoS attacks against SDN controllers, demonstrating its effectiveness through experimental analysis.	Both articles discuss identifying DDoS attacks,	Previous research focused on DDoS detection using MI and RFFI methods. Meanwhile, this research explains DDoS attacks.
IoT-based Cyber Security Management Challenges and Strategies in	The research results show that information security is a major concern for businesses around the world, with	Both articles discuss cyber security against the	The previous article explained in more detail about core IoT-based

Indonesia ((Irawan, Fadholi, Erikamaretha, & Sinlae, 2024)	information security management becoming an important challenge. Factors that influence a country's cybersecurity performance include the availability of experts, structured decision-making processes, infrastructure management, tailored security solutions, OT/IT convergence, rapid incident response, and staff training.	threat of malware and phishing attacks.	cyber security, attack trends, and device vulnerabilities, while this article does not explain as much detail as the previous article.
Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation (Shouq Alrobaian , Saif Alshahrani , and Abdulaziz Almaleh ,2023)	Research shows that the awareness of internet users in Indonesia is about the threat of phishing. Researchers found that some of the most significant demographic factors were gender. Female sources have a low level of awareness of the threat of phishing. Further action is needed to increase awareness of the threat of phishing and cooperation from all parties is needed to be able to educate about the dangers of phishing.	Both articles discuss the importance of awareness about cyber security.	The previous article focused on implementing data information security strategies and explained the methods used to measure the level of awareness of Indonesian people regarding cyber security regarding phishing threats. This article does not focus on surveys of Indonesian society.
Exploring susceptibility to phishing in the workplace (Emma J. Williams , Joanne Hinds , Adam N. Joinson ,2018)	The results of this research show the dangers of phishing emails as a means of infiltrating an organization's technical systems by encouraging employees to click on very dangerous links or attachments. Even though awareness campaigns and phishing simulations have been used, employees remain vulnerable to phishing emails.	Both articles discuss the importance of providing training to employees about phishing and spear phishing.	The previous article focused on increasing employee awareness of the inherent vulnerabilities of human resources in maintaining cyber security. This article explains the importance of employee security against phishing emails.
Overview Threats and solutions Security at Technology Internet of Things (Warsun Najib , Selo Sulistyo , Widyawan .2020)	This research shows that the Internet of Things (IoT) is the ability to connect smart objects and enable them to interact with other objects, the environment, and other intelligent computing equipment via the Internet network. The Internet of Things (IoT) has begun to be applied in many ways in various aspects of human life. From a user perspective, IoT programs have the potential to improve production, simplify the distribution of goods, and combat counterfeiting.	The two articles discuss IoT technology, not only focusing on technology device strategies, but also human resource security and various threats in the era of digital transformation.	The previous article focused on the importance of IoT in facing the challenges of digital transformation, in facing various threats from phishing attacks, fake new & service levels. Meanwhile, this article explains that IoT technology is very influential for Human Resources.

Development of Distributed Attack Prevention Denial Of Service (Ddos) On Network Resources With the integration of Network Behavior Analysis and Client Puzzle (Septian Geges, Waskitho Wibisono, 2015)	This research focuses on the issue of *web service security* . This research proposes a mechanism to secure *web services* by filtering and validating requests received to access network resources.	These two articles have similarities in finding ways to secure server networks.	This previous journal used filtration and request validation methods, while the journal we studied used the GNSD method for DDoS defense.
The Effect of Digital Transformation on the Pharmaceutical Sustainable Supply Chain Performance: The Mediating Role of Information Sharing and Traceability Using Structural Equation Modeling (Jing-Yan Ma, Lei Shi, Tae-Won Kang, 2022)	The results show that digital transformation has a significant and positive impact on sustainable supply chain performance. Sustainable supply chain. Traceability plays a mediating role. The role of mediation in is not significant. However, information sharing and traceability Different trends can have a synergistic effect that together influence supply performance. sustainable supply performance.	These two articles have in common that the progress of good and safe digital transformation is mutually beneficial for the welfare of company employees.	The difference between these two articles is that the previous journal discussed security for human resources, whereas the journal we studied focused more on system security defense strategies that encourage increased employee work awareness and awareness.
Technology Security Systems for Internet of Things Systems (Refin Refianyah Maldini , 2023)	The results show that security information systems in IoT are very important to protect information and data stored and transmitted by IoT devices. A good security system in IoT must include technology and security methods such as authentication, authorization, encryption, key management, and risk-based systems.	These two articles have in common that security in IoT is very important to protect the information sent by IoT devices.	The difference between these two articles is that the previous journal focused more on prioritizing security on IoT devices, whereas the journal we studied focused more on ways to manage security risks associated with software and firmware updates on Internet of Things (IoT) devices.

Big brother is watching you": surveillance via technology undermines employees' learning and voice behavior during digital transformation (Julia M. Kensbock, Christoph Stöckmann, 2020)	The results show that employee monitoring through technology can provide an overview of the positive impact of digital transformation on employees.	These two articles have in common the mutual increase of employee awareness of company data security.	The difference between these two articles is that the previous journal shows that digital transformation triggers employees to engage in an intrinsically motivated process in which they adopt a learning orientation, whereas our research shows that cybersecurity training for employees is very important for company integrity.
Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework (Alessandro Annarelli, Giulia Palombi, 2021)	The results suggest that the study of digitalization capabilities should not be limited to competitiveness and strategic insights, but rather include a broader perspective to fully understand its potential.	What these two articles have in common is that digital transformation requires the implementation of strong security management.	The difference between these two articles is that the previous journal is more dominant in maintaining competitiveness while ensuring safety and security, a feature for a very competitive market, whereas in our journal a comprehensive strategy is needed to face cyber security threats, such as data encryption, real security monitoring. - time, security awareness training for employees, and implementation of appropriate technology and security management solutions.

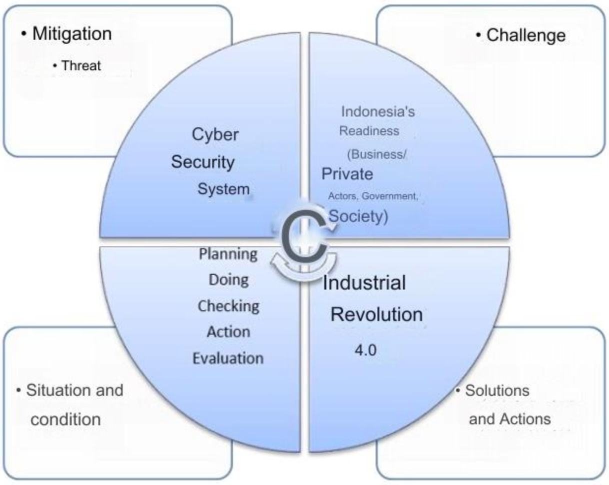

• Mitigation
• Threat
• Challenge
Cyber Security System
Indonesia's Readiness (Business/ Private Actors, Government, Society)
C
Planning
Doing
Checking
Action
Evaluation
Industrial Revolution 4.0
• Situation and condition
• Solutions and Actions

Figure 1.1 Framework for Thinking

RESULTS AND DISCUSSION

Hackers' motivations for launching malware and DDoS attacks, and how to identify, prevent, and respond effectively to attacks

Hackers who launch malware and DDoS attacks typically want to gain access to sensitive data, disrupt business operations, or exploit systems for illicit purposes. The goal is to consume system resources and cause business system failure. A DDoS attack is a DoS attack that uses multiple distributed attack sources. In general, attackers use many controlled bots (host computers/daemons, also known as zombies) spread across multiple locations to launch multiple DDoS attacks against one or more targets. With the rapid growth of botnets in recent years, the amount of traffic generated by DDoS attacks has also increased. These attacks no longer just target business servers. They also target internet infrastructure such as firewalls, routers, and domain name systems (DNS), as well as network bandwidth.

Identification of malware and DDoS attacks can be done through a number of methods such as:

a. Such monitoring is an important component of any effective cybersecurity strategy. This involves continuous observation and analysis of network traffic, system events, and other relevant data to identify potential threats and vulnerabilities. By proactively monitoring network activity, organizations can better understand their internal and external environments, detect anomalies, and take quick action to mitigate risks. It is recommended to check server logs and monitor DNS traffic to identify any anomalies.
b. Utilization of detection tools is an important aspect of the cybersecurity process. It is recommended that effective antimalware and firewalls be used as detection tools to identify and stop attacks.

c. Leveraging DNS security is an important aspect of any comprehensive cybersecurity strategy. It is recommended that DNS Security technologies such as DNS Firewall and DNSSEC be implemented to prevent attacks.

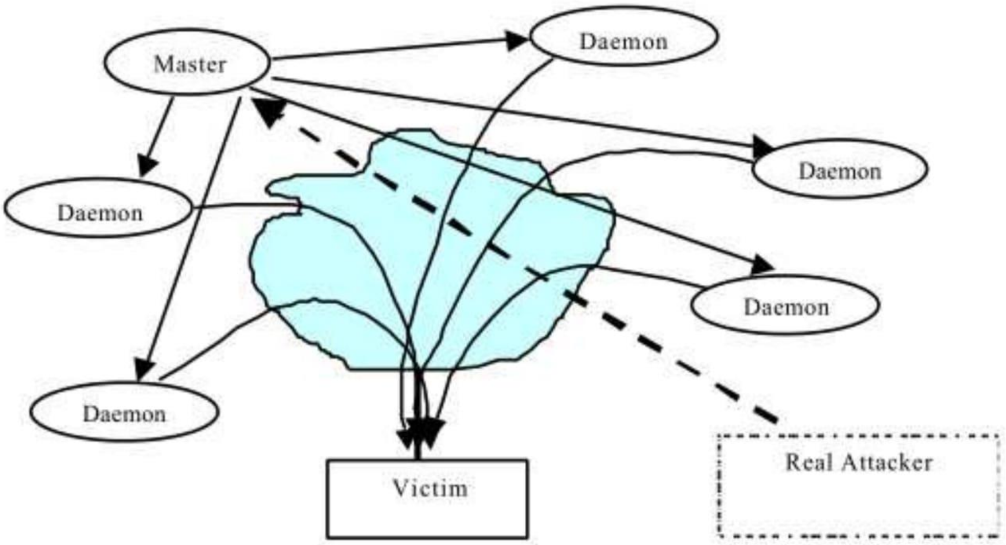
Strategies for dealing with DoS and DDoS that have been implemented

The following are DDoS defense mechanisms that have been put forward by researchers and are categorized based on where they can be applied.

1. Global Network Side Defense (GNSD) is a defense strategy designed to prevent hosts on a network from being exploited as bots to launch Distributed Denial of Service (DDoS) attacks. Two prominent examples of GNSD defenses are D-WARD [13] and BotGAD [3-5]. D-WARD monitors bidirectional traffic between internal addresses and addresses from the Internet. Active traffic statistics are stored in a network connection hash table and compared with standard models of normal traffic. Any packet traffic that does not match the flow is marked as restricted. Packet traffic limiting levels are applied dynamically, adapting to changes in traffic behavior. This is designed to facilitate rapid system recovery, allowing for the misclassification of legitimate traffic initially suspected to be part of an attack. BotGAD monitors network traffic and detects trends in bot behavior (group activity) over two consecutive time periods. If there are similarities in bot activity in the two time periods, it can be concluded that the network has been infected with bots or is part of a botnet.
2. Target Side Defense/Service Provider. Target/service provider defenses are designed to prevent the network/service provider infrastructure from exhausting its resources, thereby ensuring continued provision of services to legitimate clients. Illustrative examples of defenses using this approach include client puzzles [9] and hop count filtering [19]. The client puzzle relies on validation of the client requesting services from the server. This method requires the client to solve a puzzle to access the services provided by the server. Puzzles can be mathematical calculations, cryptography, or other problems that require resource consumption (e.g. CPU and memory) on the client to solve. Hop count filtering validates packets by counting the packet's hop count and comparing it to the database hop count when the network is in a normal state (i.e., no attacks have occurred). Wang et al. proposed a hop count filtering mechanism based on the observation that most spoofed packets do not have hop count values consistent with the spoofed addresses used. As a result, the time-to-live (TTL) value in a packet can be used to determine whether the packet is fake. The router subtracts the TTL from the IP address of the packet it is traversing before forwarding it to the next hop. The final TTL value when a packet reaches its destination is the initial TTL value minus the number of hops traversed (i.e. the number of hops).

Although the main perpetrator of a distributed denial of service (DDoS) attack is usually considered solely responsible for issuing execution orders, in reality, he must also be involved in the planning to ensure the success of the attack. For an attacker to successfully compromise the daemon, they must first gain access to all computer hosts and networks on which the daemon will be installed. Before launching an attack, an attacker must study the target network topology to identify potential vulnerabilities and system tendencies that can be exploited to launch an attack.

The following are defense mechanisms against DDoS that have been proposed by researchers and categorized based on the context in which they can be applied.(Geges & Wibisono, 2015)



Picture. 1. Illustration of a DDoS attack

The Impact of Not Providing Training to Employees on Cybersecurity Regarding Phishing and Spear Phishing Attacks

The consequences of not providing cybersecurity training to employees regarding phishing and spear-phishing attacks can be devastating. One of the main reasons for the increase in phishing attacks is lack of employee awareness and training. Employees who are not aware of the techniques and characteristics of phishing attacks are more vulnerable to these attacks. Without training, employees lack the ability to recognize and anticipate attacks, making them more vulnerable to fraud and loss of sensitive data.

Lack of training can also lead to alert fatigue, where cybersecurity professionals have to manage many alerts in a limited time, leaving them without enough time to effectively validate each alert. This can result in some alerts being invalid, such as false positives, which can disrupt security operations and consume resources ineffectively.

Another impact of not providing training is the loss of sensitive data and damage to the company's reputation. Phishing attacks can steal confidential or sensitive information, such as passwords or financial details, which can have serious consequences for an organization. Additionally, phishing attacks can damage a company's reputation if customer data is stolen or systems are compromised, resulting in negative publicity and loss of customer trust.

Therefore, regular employee training on cybersecurity, including phishing and spear-phishing attacks, is critical to maintaining the integrity, confidentiality and availability of information in the business environment. This training can increase employee awareness of the techniques and characteristics of phishing attacks so they can better identify and anticipate attacks, reducing the risk of losing sensitive data and damaging the company's reputation.

How to manage security risks associated with software and firmware updates on Internet of Things (IoT) devices distributed across a network

Managing security risks associated with software and firmware updates on Internet of Things (IoT) devices distributed across networks requires an integrated and sustainable strategy. Here are some steps you can take to manage security risks:

- Update Management: Ensure that IoT devices have an effective update management system, allowing current and secure software and firmware updates to be downloaded and installed regularly. These systems must be able to detect and address security issues related to out-of-date software and firmware.
- Network Monitoring: Ensure that the network used to connect IoT devices has strict monitoring, including access monitoring, traffic monitoring, and data monitoring. This can be done using technology such as firewalls, intrusion detection systems, and encryption.
- Use of Security Protocols: Ensure that IoT devices use up-to-date and secure security protocols, such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL), to encrypt data sent over the network. This can help prevent man-in-the-middle attacks and data theft.
- Device Monitoring: Ensure that IoT devices have strict monitoring, including access monitoring, traffic monitoring, and data monitoring. This can be done using technology such as access control, intrusion detection systems, and data encryption.
- Risk Management: Ensure that IoT devices have an effective risk management system, which enables detection and response to potential security risks associated with software and firmware updates. This can be done using technology such as risk assessment tools and incident response plans.

  User Oversight: Ensure that IoT device users have a heightened awareness of the security risks associated with software and firmware updates. This can be done by providing training and clear information about IoT security.

- Vendor Oversight: Ensure that IoT device vendors have strict and transparent security policies, and have effective risk management systems. This can be done by conducting research and evaluating the security of the device before purchasing.

By following these steps organizations can manage security risks associated with software and firmware updates on IoT devices distributed across the network, as well as ensure the security and integrity of data collected by IoT devices.

CONCLUSION

In the current era of digital transformation, implementing security management or information security is very important. Cybersecurity threats such as malware, phishing attacks, DDoS, and others are increasingly complex and can threaten data security and the continuity of organizational operations.

Comprehensive strategies are needed to deal with cybersecurity threats, such as data encryption, real-time security monitoring, security awareness training for employees, and implementation of appropriate technology and security management solutions. Training and increasing cybersecurity awareness for employees is essential to prevent human errors that can result in data leaks or security attacks.

Human resource security management, such as careful hiring, training, and strict security policies, also plays an important role in protecting an organization's sensitive information. Digital transformation raises new security challenges, such as the security of Internet of Things (IoT) devices that need to be managed well through secure software/firmware updates and strict network monitoring.

Collaboration between government, the private sector and society is needed in efforts to improve overall cyber security, as well as develop adequate security regulations and standards. Overall, implementing comprehensive security management involving technology, human resources, regulations and cross-sector collaboration is very important in the current era of digital transformation to protect information assets and maintain organizational business continuity.

Suggestions for further research can be added in more detail and specifically to discuss topics similar to this research.

REFERENCE

AVKalpana, D. Digvijay, R. Chenchaiah, & C. SaiVignesh. (2021). Implementing Cybersecurity in IoT Using IPAI Algorithm.

Adhiaksa, AR (2021, April). Simple steps to secure your device from hackers.

Admin. (2023, June). Security in the Internet of Things (IoT): Challenges and Solutions.

Alrobaian, S., Alshahrani, S., & Almaleh, A. (2023). Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation.

Annarelli, A., & Palombi, G. (2021). Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework.

Arman, M. (2020). Web Server Defense Method Against Distributed Slow HTTP DoS Attack.

Disemadi, HS (2021). The Urgency of Special Regulations and the Use of Artificial Intelligence in Realizing Personal Data Protection in Indonesia.

Eijikman, Q. (2013). Digital Security Governance and Accountability in Europe: Ethical Dilemmas in Terrorism Risk Management.

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behavior as an aspect of cybersecurity assurance.

Geges, S., & Wibisono, W. (2015). Development of Prevention of Distributed Denial of Service (DDoS) Attacks on Network Resources by Integrating Network Behavior Analysis and Client Puzzle.

HRF. (2022). Risk Management Framework that Companies Must Implement.

Ikhsan. (2023). Digital Transformation and its Impact in Indonesia.

Irawan, A., Fadholi, WH, Erikamaretha, Z., & Sinlae, F. (2024). IoT-based Cyber Security Management Challenges and Strategies in Indonesia.

Jasmina M. Veličković, K. J. (2023). CYBERATTACKS ON HEALTHCARE SYSTEMS.

Kensbock, J. M., & Stockmann, C. (2020). Big brother is watching you": surveillance via technology undermines employees' learning and voice behavior during digital transformation .

Khoironi, S. c. (2020). The influence of analysis of cyber security culture training needs as an effort to develop competency for state civil servants in the digital era.

we p. (2024, January). Latest Cyber Security Developments in Indonesia.

Ma, J.-Y., Shi, L., & Kang, T.-W. (2022). The Effect of Digital Transformation on the Pharmaceutical Sustainable Supply Chain Performance: The Mediating Role of Information Sharing and Traceability Using Structural Equation Modeling.

Maldini, R.R. (2023). Technology Security System for Internet of Things Systems.

Maldini, R.R. (2023). Technology Security Systems for Internet of Things Systems.

Maya Utami Dewi, SM (2022). Securing Internet Of Things (IoT) Devices.

Munandar, A. (2023). *SPBE Security in Digital Transfirmation.*

Muslim, Sephira, A., Abrar, MH, Angin, SL, & Hidayatullah, H. (2024). Cyber security analysis in the digital era "security challenges and strategies".

Najib, W., Sulistyo, S., & Widyawan. (2020). Overview of Security Threats and Solutions in Internet of Things Technology.

Oktafiani, C. (2020). MANAGEMENT INFORMATION SYSTEM "Information Security in the Use of Information Technology at PT.

OuhssiniA, M., AfdelA, K., AgherrabiB, E., AkouharC, M., & AbardaD, A. (2024). Deepdefens: A comprehensive framework for DDoS Attack detection and prevention in computing.

Latest Cyber Security Developments in Indonesia. (2024, January).

Purbo, O. (2023, May). *Cyber Security: Emergency Response and Disasters* .

Putra, FP, Dewi, SM, Maugfiroh, & Hamzah, A. (2023). Privacy and Security Application of IoT in Everyday Life Challenges and Implications.

Rayhan, M., Alfaridzi, MD, Saputra, IE, & Sinlae, F. (2023). Implementation of security management to prevent fraudulent online sales transactions on buying and selling forums (Facebook).

Cyber, B.K. (2022). AI and Automation Help Prevent Ransomware and Phishing Attacks.

Solorzano, G. A., Gutiérrez, A. F., & Gordillo, A. P. (2023). Data Security Threats On Smart Devices At Home. *ARPHA Conference Abstracts* .

Triwahyuni, D., & Wulandari, TA (2016). United States Cyber Security Strategy. *Journal of Political Science and Communication* .

Tulungen, EE, Saerang, DP, & Maramis, JB (2022). Digital Transformation: The Role of Digital Leadership.

Main, L. (2023, December 1). 5 main causes of data leaks.

widya. (2024). Protect Data From Phishing in 2024.

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to Phishing in the workplace.