Iraqi Journal of Information and Communications Technology(IJICT)
Vol. 6, Issue 2, August 2023

www.ijict.edu.iq

ISSN:2222-758X
e-ISSN: 2789-7362

ZERO TRUST SECURITY MODEL FOR ENTERPRISE NETWORKS

Rania M. Habash [1], **Mahmood K. Ibrahem** [2]
[1,2] College of Information Engineering, Al-Nahrain University, Baghdad, Iraq
rania.mustafah1997@gmail.com [1], mahmoodkhalel@coie-nahrain.edu.iq [2]
Corresponding Author: Mahmood K. Ibrahem
Received:13/08/2022; Revised: 12/11/2022; Accepted:06/04/2023
DOI:10.31987/ijict.6.2.223

***Abstract*- Zero Trust (ZT) is security model and follow the concept of ânever trust, always verifyâ. ZT require to strict identity verification for devise and clients trying to access recourses on private networks regardless of whether they are sitting within or outside the networks. As opposed to perimeter-based architecture, which makes the assumption that all internal network parties are trusted and all external network parties are untrusted. In enterprise network the internal network parties is automatically seen as trusted entities granting them access to network resources. The insider threat actor has been successful in exploiting their access. So that, enterprise networks become more exposed to inside and outside threads. As a result, we need to add the zero-trust principle to the enterprise network to protect it from the inside. In this paper, the ZT model, is assumed inside the militarized zone. There may be a threat to the sensitive data. Any internal company network users cannot manipulation on his computer without permission from the administrator this is done by the group policies that have been implemented in ZT. This model has been shown to be quite effective in protecting the sensitive data against unauthorized access and also the manipulation by the insider user. Following that, an attack originating from inside of the network was launched against the enterprise and zero trust network. In the enterprise network, the network was effectively attacked, and the attack's validity was also increased to fully penetrate the enterprise. The attack did not succeed in the zero-trust network because the attacker cannot pass the User Account Control (UAC) to gain the NT authority.**

keywords: **Zero Trust model, Zero Trust security, Enterprise network, Cybersecurity, Never trust.**

I. INTRODUCTION

Traditionally, enterprise Information Technology (IT) networks have been closed networks with external access restricted to network edge locations [1]. Segmentation and security have been established within the corporate network by isolating IT services from user segments and establishing access control between them [2]. Controlling traffic inside different networking locations has frequently been used to add additional security [3]. Internal services are accessible once you have access to the company's internal network, which is regarded as a critical part of security controls. This was a valid design principle in the past, when services were largely housed in internal locations or datacenters [4][5]. The majority of businesses now use a growing number of cloud services, making it hard to safeguard access end-to-end using simply network-based access control methods [6]. Due to the fact that businesses are migrating an increasing amount of workloads to the cloud, IT services are frequently dispersed over numerous private and public datacenters [7]. Users are also no longer restricted to corporate Local Area Networks (LANs); instead, they are mobile and frequently linked simply via the internet or Virtual Private Network (VPN) services [8].

Enterprise networks are getting more and more decentralized as a result of how IT services are used nowadays [9]. It is frequently impractical to detect location or have similar network-based access controls in placefor cloud-based services as it was previously [10][11]. In order to solve this issue, zero trust architecture eliminates the idea of trust from the network itself [12]. Every network is viewed from a service perspective as an external network. This indicates that the network address or the location is no longer a factor in determining who gets access to these services [13]. Networks are viewed in

ISSN:2222-758X
e-ISSN: 2789-7362

Zero Trust Architecture more as a means of connecting the users to the services. Access control and identity verification are both implemented in supporting systems or within the service itself [14]. The network as the primary security enforcement point is still no longer adequate; access to the company's internal network should no longer imply access to services. Identity is becoming increasingly significant [15]. It is claimed that Zero Trust is a solution that improves security. It is also claimed to reduce the complexity of security control implementations. Fewer controls translate into fewer systems to set up, maintain, and keep updated, which might lead to a reduction in the cost of security mechanisms among most enterprises [16]. Also, The placement of the security solutions is designed to be more straightforward and effective than with traditional network security solutions [17].

The perimeter-less design, often known as zero trust, means that rather than using a single or a small number of global perimeters to secure the network, ZT generates the perimeter(s) for each network user separately based on its identity by developing an overlay that decides whether the network access is permitted or not [18]. Zero Trust, on the other hand, cannot be added to an existing network without completely rebuilding the entire network security architecture. Both new security components and existing ones must be removed to implement zero trust [19]. With this reorganization, it is expected that the Zero Trust will render some infrastructure components unnecessary and enable the removal of some of the perimeter security measures used in traditional network designs [20]. To demonstrate how ZT networks are different from traditional network architectures, the paper also aims to highlight the differences between ZT networks and traditional networks in general. Security measures are the paper's main topic, and it explains how the difference between these two types of network implementations. The following provides an overview of related research:

In [21], this study defines the design of the policy enforcement framework of Zero Trust Network (ZTN), which tackles many of the open challenges related to risk-based access management. One of the fundamental policy languages and a mapping mechanism is a generic firewall policy. These regulations must be implemented on the firewall and written in a particular firewall syntax. They demonstrate the validity of this approach using a simple proof-of-concept.

References [22] and [23] both mentions how to provide fine-grained access control to the system by proposing different architecture that based on authorization systems and can detect the great majority of data security vulnerabilities. eZTrust, a network-free microservice perimeterization method, was put out by [24]. Data center operators may securely and effectively apply such policies in a completely network-independent manner, which enables data center tenants to specify access control policies based on their fine-grained workload. The viability of their strategy is determined by the implementation of a proof-of-concept prototype. They discovered that eZTrust has a 1.5-2.5 times lower CPU overhead and a 2-5 times lower packet delay than conventional perimeterization solutions.

In [25], the idea and use of a zero-trust architecture are described. There are some difficulties with Zero Trust Architecture (ZTA) that are discussed and examined, such as issues with vendor lock-in or a lack of standardization. A summary of stages and topics to consider when migrating from perimeter-based architecture to ZTA is presented at the end.

In [26], the authors offered a novel approach to the Zero Trust Model (ZTM) for granting access control to sensitive information. For internal or external network partners, ZTM does not provide a default level of trust. To secure sensitive

ISSN:2222-758X
e-ISSN: 2789-7362

data, new policies have been adopted in ZTM. Critical data is very well protected from illegal access using this strategy. The above-mentioned research efforts were focused on how to protect the network from insiders. To solve the problem of hacking that results from trusted people who are within the network in the traditional network, a ZTM was built in this paper for the purpose of preventing network penetration from occurring from the inside and not only from outside the network.

The rest of the paper is organized as follows: The proposed architecture of the Zero Trust network is described in Section II. The results of the proposed architecture and how it improves the security of the network are introduced in Section III. Section IV of the paper concludes the paper.

II. The Proposed Architecture

First, enterprise networks were implemented by using the Emulated Virtual Environment-next generation (EVE-NG) emulation. EVE-NG gives users access to tools for communicating with and connecting to virtual and real devices. Numerous EVE-NG qualities significantly improve usability, reusability, manageability, interconnection, distribution, and subsequently the ability to comprehend and share topologies, work, and concepts. This simply means it will take less time and money to set up what you need. Enterprise networks consist of the following areas: campus, data center, internet edge, demilitarized zone (DMZ), and a firewall. Fig.1 illustrates Enterprise networks.

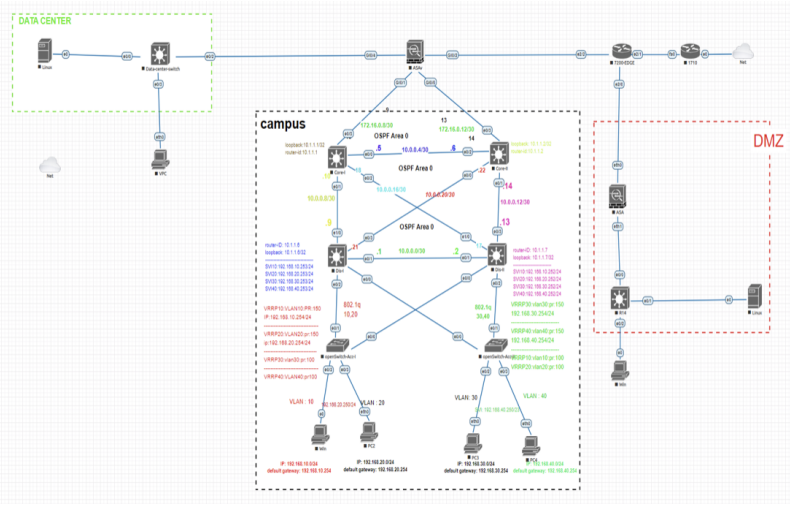

Figure 1: Enterprise Network

Based on their functions in the networks, the campus network is divided into three layers. The first layer is the access layer, which provides VLAN access and gives the user access to the network. The next layer is the distribution layer, which provides the policy-based connection, aggregates all closet access switches, and manages access control, Quality of service (QoS), and route redundancy. The last layer is the core layer, and its function is to provide connectivity between different campus network sections and the rest of the network. For business continuity and disaster recovery, the enterprise uses an off-site data center. Utilizing highly accessible WAN services, the campus is linked to the remote data center. The

ISSN:2222-758X
e-ISSN: 2789-7362

enterprise data center (DC) architecture consists of three primary layers: the access layer, the aggregation layer, and the core layer.

The Internet edge connects the components of the internal enterprise network to the Internet and acts as the gateway. In addition, it is widely employed to deliver inbound connections, such as remote access to the network, and also publish services in the DMZ to the Internet. Security measures at the Internet edge protect the trusted company network from external, untrusted networks such as the Internet.

A network's security is significantly increased in a demilitarized zone (DMZ). The DMZ adds an additional level of security to the network. It is also used to protect sensitive data. The DMZ isolates the internal network from the external network. It is done by separating machines that can be readily accessed by other machines from one another.

Firewalls are devices that regulate network traffic across hosts and networks with various security postures. The firewalls are used to prevent illegal access to the devices and services in the enterprise.

The user is regarded as a trusted individual and can access the services and many different network regions once their identity has been confirmed and access to enterprise resources has been granted. And this is the issue where it's possible that one of the insider employees of the company who has access to the sources is a harmful person who compromises the network's security. To solve this issue, the concept of Zero Trust (ZT) was added to enterprise networks, which dictates that both the outside and inside are untrusted. ZT is a set of ideas and concepts enhancing network security that can be utilized by the network in a way that meets its requirements. In this proposed architecture, the company's need is to make the insider user, even if he is trusted, unable to change, add, or delete anything from the network or use any of the removable storage access.

The only way he can do this is with permission from the administrator of the network. To add the concept of ZT to the enterprise network, we use Active Directory (AD) that is based on Windows Server 2016 on the network, and through the policy group, a set of actions was identified to make the insider user unable to make any changes within the PC. The directory holds important data about the environment, such as the number of users and computers and who is authorized to do what. The services in an IT environment are in charge of a sizable amount of the operations. They precisely authenticate each user, usually by checking the user ID and password they enter, to ensure that they are who they claim to be and only allow them access to the data they are permitted to use.

To connect the user's PC with the server that is based on the AD, the settings of the user PC need to be changed from the workgroup to the domain "local.com". After that, the username and password of the administration are entered, which can manage and control the network, as shown in Figs. 2 and 3. Administration permission is required from the user who needs to take action. To obtain admin permission, the user must know the username and password of the administration, which are only known by the administration.

Today, it is more difficult to compromise a network perimeter. Because it has better network architecture (subnets,VLAN, DMZ, Quarantine Network, etc.), Server hardening, and AV, IDS, IPS, UTM, Firewalls NexGen, etc. So,we will exploit the Client-side, and this type of security breach requires user interaction in order to be triggered (open a link, an executable file, etc.). The reason for that is that the user has access to the network, system, data, and internet from inside the network.

ISSN:2222-758X
e-ISSN: 2789-7362

Which makes it easier for us to penetrate. Post-exploitation is the last technicalstage of the penetration testing process. The first task to perform is Privilege escalation and maintaining Access. Once we have built our way into the victim machine, we can move on to the next phase of post-exploitation data harvesting. The main purpose of the next step is to map the Internal organizations in order to find other Exploitable machines to get closer to our goal. The last step is the exploitation of the new system and pivoting.

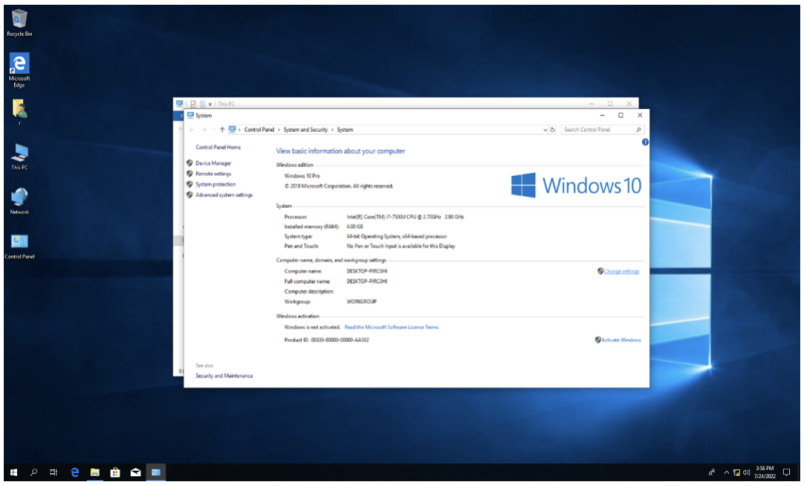

Figure 2: User Interface

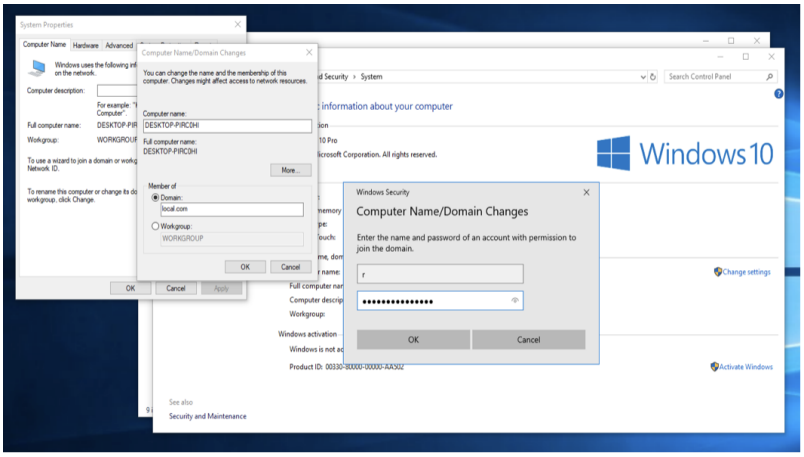

Figure 3: User Connected to AD

III. Results and Discussion

This network is an illustrative and simplified part of the network that was previously explained in the previous section. This network was created to demonstrate the difference between a traditional network and a Zero-Trust network in terms

ISSN:2222-758X
e-ISSN: 2789-7362

of security by launching an attack on the PC that connects with the access switch and also on the PC that connects with AD. Fig. 4 illustrates the attacked network.

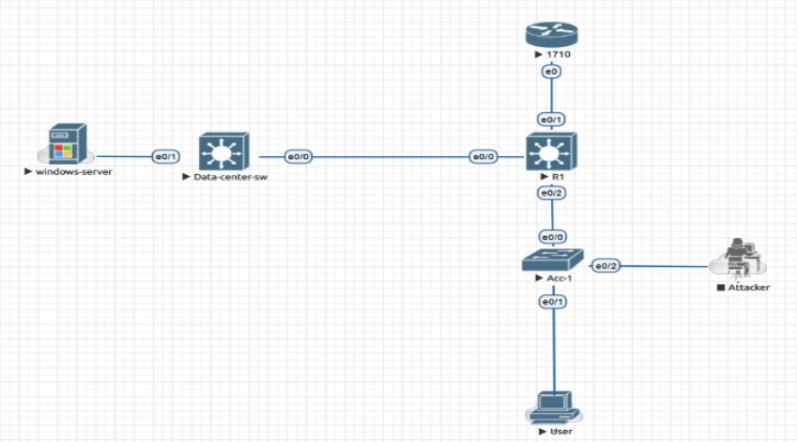

Figure 4: Illustrative Network With Attack

Because Kali Linux is used for hacking activities, the virus was constructed using it. msfvenom was used to construct our shell code, which refers to the creation of a shell that enables the execution of any code the attacker desires.

```
msfvenom -p windows/meterpreter/reverse_http LHOST=x.x.x.x LPORT=443
EXITFUNC=thread -f vbapplication
```

After that, the virus is generated in encoder form, so only the RAM can understand it, as shown in Fig. 5.

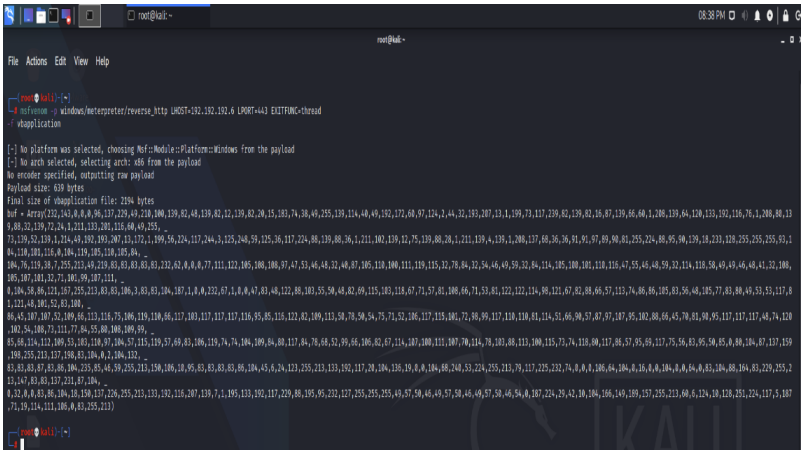

Figure 5: Generation of Virus

To create the virus in the Word document, the shell code will be inserted into the document through the macros. A macro is a collection of commands and instructions that users arrange together to perform a task automatically. And then,

ISSN:2222-758X
e-ISSN: 2789-7362

this document will be sent to the victimâs PC. The hacking process will take place if the user receives and opens this Word document. Fig. 6 shows the addition of the virus to a Word document.

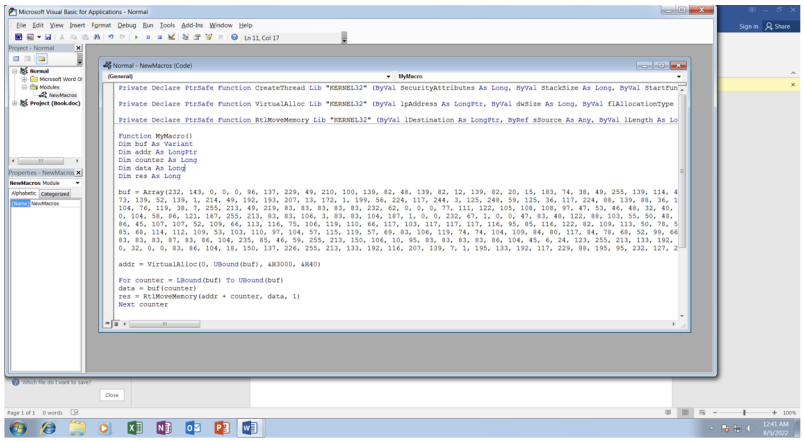

Figure 6: Adding the Virus to Word

One of the most popular penetration testing tools is the Metasploit Framework, an open-source modular framework used to attack systems to look for security vulnerabilities, and it is included with Kali Linux. The command to start Metasploit in Kail Linux is msfconsole. The Multihandler tool that is inside the Metasploit will be used and define its own settings, and set payload windows/meterpreter/reverse_tcp which means it connects to a listener on the attacker's machine. Set lhost and give the IP of the attacker and also the port will be set and finally the exploit to start the session with the victim's computer. And then the payload will automatically get back to you as soon as you set up the handler again. So that it becomes responsible for receiving the connection with the victim's computer. Fig. 7 illustrate the multi/handler.

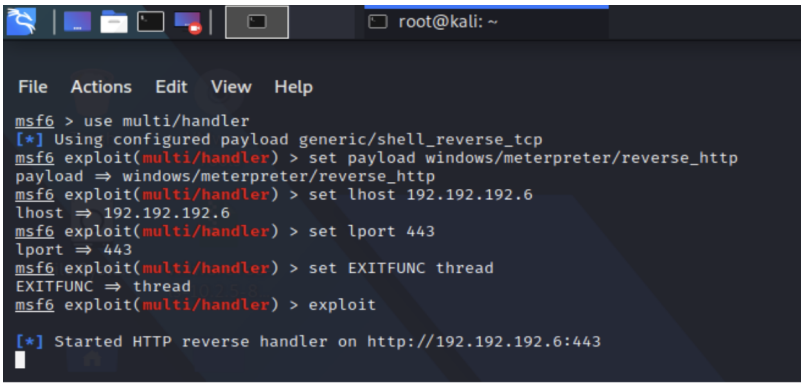

Figure 7: Multi/Handler

When the victim opens the Word document, the session between the attacker and victim is open, and the attacker gains information about the victim's computer through the sysinfo, as shown in Fig. 8. That shows us the type of the victim's

ISSN:2222-758X
e-ISSN: 2789-7362

computer and the operating system that is running on it, as well as the language and number of the account that is logged on it.

Figure 8: Information About Victim

Now that the hacking procedure has been completed successfully on the victim's computer, the attacker needs to gain additional authority within the victim's computer to gather data about the organization's network because their overall purpose is to hack the entire organization. Meaning that the attacker gets the NT Authority System, which enables the attacker to manage the users and groups, launch device drivers, and initiate and terminate services, among others. It can do any system task and has extensive rights. The attacker is neither an admin nor a system, and only User Account Control (UAC) is enabled. The attacker must pass the UAC by, as shown in Fig. 9. By limiting application software to regular user privileges until an administrator approves an increase or elevation. It aims to enhance the security of Microsoft Windows. In this manner, malware is prevented from infecting the operating system, and only applications trusted by the user may be granted administrator access.

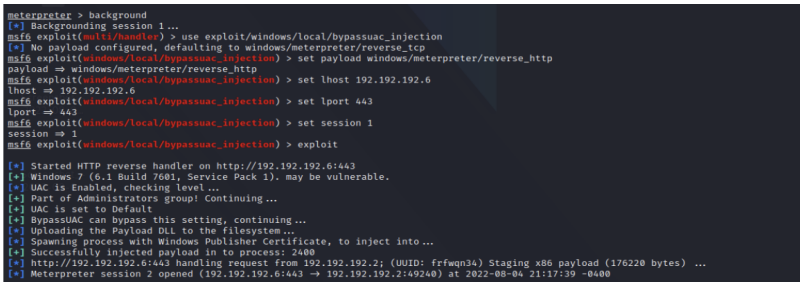

Figure 9: Pass the UAC

The attacker, after passing the UAC, gained the NT authority system, and since the UAC is not enabled, the attacker now became the administrator and system. He can collect information about the rest of the computers and the network in some way. That is, the entire site was hacked. Fig. 10 illustrates traditional network penetration.

Figure 10: Success Of the Traditional Network Penetration

ISSN:2222-758X
e-ISSN: 2789-7362

Now, we will try to attack the user's computer that is connected to the Active Directory Windows server. Because of the attackerâs inability to pass the UAC, no session between the attacker and any one of the users located inside the company was created. So, the penetrant process will fail with the ZT, as shown in Fig. 11.

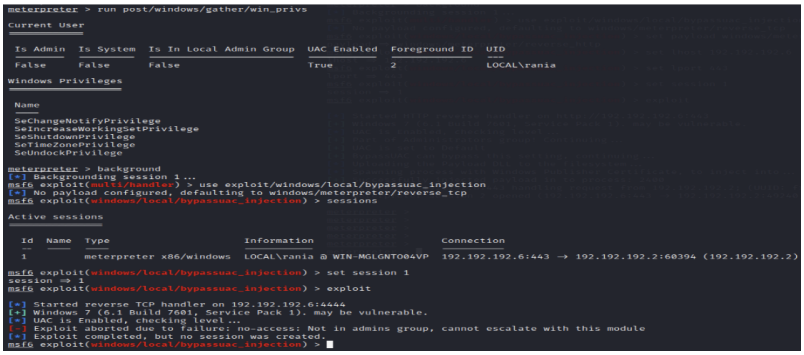

Figure 11: Failure Of the Zero Trust Penetration

As a result, one can say that the model of ZT will solve the intruder's problem, but delay will result in completing daily transactions and tasks. The focus was on security and how to protect the system from internal threats. but the problem of delay can be solved by adding more than one server that performs the investigation of users.

IV. Conclusion

In this paper, the enterprise network and the ZT concept were designed to enhance security within the organization. Taking into consideration that people within the organization's perimeter are also untrusted because they can manipulate and access network resources within the traditional network, Active Directory implemented the ZT concept, and people inside the organization were restricted. The network was compromised by attacking one of the users inside the organization's perimeter; however, the zero-trust principle helped prevent the hacker from breaching the user inside the organization's perimeter. Consequently, the zero-trust objective of enhancing the network's security from the inside, where attackers may exploit it, was accomplished.

Funding

None

ACKNOLEDGEMENT

The author would like to thank the reviewers for their valuable contribution in the publication of this paper.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

References

[1] S. Arivazhagan, D. Rengamani, J. Poongavanam, "Inspiring Enterprise Resource Planning To Information Technology Networking Springs in Apprehension of Human Resource., PalArch's Journal of Archaeology of Egypt/Egyptology, vol. 17, no. 9, 2020.

ISSN:2222-758X
e-ISSN: 2789-7362

[2] National Security Agency "Embracing a zero trust model," ver. 1.0, cypersecurity & infrastructure security agency, 2021.
[3] L. Zhu, "Analysis and Research of Enterprise Information System Security Based on e-Commerce," Academic Journal of Computing & Information Science, vol. 3, no. 3, 2020.
[4] D. Nadig and B. Ramamurthy, "Securing large-scale data transfers in campus networks: Experiences, issues, and challenges," Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, New York, USA, 2019.
[5] A. Alchinov, Z. Tavbulatova, O. Dudareva, and M. Ivanov, "Modern approach to enterprise information systems," Journal of Physics: Conference Series, vol. 1661, no. 1, 2020.
[6] V.Jakkal âZero Trust Adoption Report Cybersecurity Insiders,â accessed: 2022/8/11, https:/query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWGWha
[7] P. Yang, N. Xiong, and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," IEEE Access, vol. 8, 2020.
[8] I. Dumitru, "Zero Trust Security," Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3), vol. 9, 2022.
[9] L. Bakos and D. Dumitrascu, "Decentralized enterprise risk management issues under rapidly changing environments," Risks, vol. 9 , no. 9, 2021.
[10] R. Sharma, "Handbook of: Data Center Management," 1st Edition, Auerbach Publications, 2017.
[11] B. Sreeja, M. B. Saleem, and V. Sravya, "Issues With Perimeter Based Network Security and a Better Model To Resolve Them," European Journal of Molecular & Clinical Medicine, vol. 7, no. 9, 2020.
[12] P. AssunÃ§Ã£o, "A Zero Trust Approach to Network Security," Proceedings of the Digital Privacy and Security Conference, Porto, Portugal,2019.
[13] J. Heary, "How to approach a Zero Trust security model,", CCIE #7680, Cisco Live, barcalona, 2020.
[14] M. Campbell, "Beyond Zero Trust: Trust Is a Vulnerability," Computer, vol. 53, no. 10, 2020.
[15] Fortinet, "Zero-trust Solutions for Comprehensive Visibility and Control," 2021, accessed: 2022/8/11
[16] ACT-IAC Zero Trust Project Team, "Zero Trust Cybersecurity Current Trends," 2019, accessed: 2022/8/11, https://www.actiac.org/ system/files/ACT-IAC Zero Trust Project Report 04182019.pdf
[17] C. Cunningham, J. Pollard, and D. Holmes, âThe eight business and security benefits of zero trust," Forrester Reseach Novemb. 2019.
[18] A. Woland, "Five Steps to Perimeter-Less Security," CCIE #20113, cisco live, barcalona, 2020.
[19] S. Rose, A. Kerman, and O. Borchert, "Implementing a Zero Trust," National Institute of Standards and Technolog, 2020.
[20] S.Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, Special Publication 800-207, 2020.
[21] W. Naeem and S. McLoone, "Welcome to the 29th irish signals and systems conference (ISSC 2018)," 29th Irish Signals Syst. Conf, Belfast, United Kingdom, 2018.
[22] T. Yang, Z.Lei, and P. Ruxiang. "Fine-grained big data security method based on zero trust model," 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, 2018.
[23] Q. Yao, Q. Wang, X. Zhang, and J. Fei, "Dynamic Access Control and Authorization System based on Zero-trust architecture," 2020 International Conference on Control, Robotics and Intelligent System, Xiamen, China, 2020.
[24] Z. Zaheer, H. Chang, S. Mukherjee, and J. Merwe, "EZTrust: Network-Independent Zero-Trust Perimeterization for Microservicces," Proceedings of the 2019 ACM Symposium on SDN Research, San Jose, CA, USA, 2019
[25] S. Jeerakanok, T. Uehara, and A. Inomata, "Migrating to Zero Trust Architecture: Reviews and Challenges," Security and Communication Networks, vol. 2021, 2021.
[26] I. Ahmed, T. Nahar, S. Urmi, and K. Taher, "Protection of sensitive data in zero trust model," the International Conference on Computing Advancements, Dhaka, Bangladesh , 2020.

