Project Proposal Document

**Project Proposal document**

Introduction

Computer network is a backbone of modern-day communications whether it is a simple email or sharing resources like storage, printer etc. (Kizza, 2005) defines computer network as a distributed system consisting of computers that are interconnected through a medium. It can be wired or wireless depending on needs. Security is a very important aspect of networks. As networks allow to access multiple devices across the globe or different locations it is important to place controls that allow only authorized personals to access the network. To protect networks from unauthorized access many techniques and controls were developed and put in place to ensure safety of all. Due to advancement of knowledge and research many techniques were made as a standard to uphold a certain level of security with the option to add more should the need arise. In 1960s when networks were rapidly spreading, governments, military and public sectors were establishing networks many incidents were witnessed where data was stolen, or system was rendered useless because of very little or no security at all. By 1980 the networks had spread across the entire world, and it was known as internet and as a result the threats rose to an exponential number. Government agencies worked with other users of network to develop CERT Computer Emergency Response Team to mitigate the threats and research way to prevent such attacks (radware.com). With the increase in technological advancement more sophisticated controls are being placed to strengthen the security of networks but here is a limit to how much security can be placed on existing networks. It is essential to take security controls in account when designing a network rather then design a network and then implement security when it comes under attack. According to (Patnaik, 2021) It is mandatory to consider the following when developing a secure network:

1. Confidentiality: Means that information should be held private
2. Integrity: Ensure that the data is correct, and no alterations has occurred.
3. Authentication: To verify that users are who they say they are.
4. Access: Only authorized users can have access to the resources.
5. Non-repudiation: Ensure that users can not deny the use of network.

Network security can be enhanced by assessing the company’s attack surface meaning that how many assets does the company has and what are the access points. Identifying the risks and then combining the security solutions to come up with a design to secure the assets based on their priority or likely hood of getting attacked is a good way to develop a strategy to counter any attacks against a network. As stated by (Dowd, McHenry, 1998) “With the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack an effective network security plan is developed.”

**Aims and Objectives**

The aim of this project is to design a secure network that prevents intrusion and data loss with the help of several network security controls.

Objectives

* Identify the risks and classifying the assets on priority basis.
* To analyze and find the best principles to implement for secure network design.
* Implementation of Network segmentation
* Analysis of monitoring tools and use the ones best suited for our needs.
* Testing the network and provides its capabilities and limits.
* Preparing documentation and recommendation.

**Tasks**

1. List down assets and resources and set their priorities.
2. Design the actual network
3. Apply Network Segmentation
4. Test IPS and data loss prevention tools in virtual environment and place them on junctions.
5. Develop firewall rules and test them against different attacks.
6. Testing the entire connectivity of the network.

It is important to identify the resources we need to protect in order to place security controls. Dividing network into smaller junctions so that even one junction is penetrated other junctions remain unharmed and still keeping resources safe. Intrusion prevention and data loss prevention controls monitor the traffic and detect any unauthorized access and block it. Data loss prevention control ensures that data is not lost or misused. Firewall ensure that only specific requests are allowed into the network and others will be denied.

**Resources**

In order to design the network and test its capabilities there are some sources that are required.

Diagramming tools

I need to find and select the best diagramming tool or network mapper that will be used to show the entire network. It will be used to virtual lay down the entire network and test some degree of its connectivity and capabilities. Some tools even allow to place any controls and monitoring tools as well so it will be very useful.

Monitoring tools and firewall

There are many monitoring tools available, but I need to keep in mind the ones best suited for small level organization and cost effective. Some tools may even combine the features of others so it can be helpful in cutting the cost. Incase of firewall it all depends on the rules, there is not much difference in capabilities of different vendors.

Virtual environment

It will be very useful in testing the features and limits of tools and firewall rules we can attempt attacks and try to bypass the security checks to ensure that the controls are working the way we want them to.

**Project Risks**

During the development of this project, we can assume some risks that can affect the outcome or cause the project completion delay. Some

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Description | Scale | Solution |
| Accidental damage to computer or loss of data | It is possible to get the system damaged or stollen which was being used to carry out the project. | Low | Keep back up in cloud or separate external hard drive to ensure nothing goes wrong. |
| Tools may not be compatible with network configuration or combination with other tools. | Some tools have some bugs or dependencies that can cause them to deteriorate or not perform as expected. | Medium | Gather as much information about them as possible and look for reviews before hand to avoid using such tools or find a fix for them to work. |
| Insufficient knowledge of the task | It is likely to encounter a situation I have very little knowledge of, and it may halt the progress. | Medium | In this case first discuss with supervisor and look for professionals or experts that have specialties in that area and ask for their advice. |
| Increased or additional requirements that are added later on | Client may add some additional requirement and making room for it during the project can disrupt the timeline. | Medium | Discuss with the supervisor and look into the details and adjust them accordingly. |

**Professional Issues**

The project will be completed under the supervision of assigned supervisor and taking ethics legal issues into account, and it will be developed with software and information freely available. It will be used for academic purposes and provide recommendations with its limits and abilities.

**Time Plan**

Timeline, waterfall chart

Description automatically generatedThe project is divided into tasks and assigning time to each tasks helps devise a plan to complete them in time.

Updated Literature Survey

**Introduction**

Internet is vast collection of networks in which millions of computers communicate using some set of rules also known as protocols. Internet is expanding steadily over the time (Mowery et al. 2002). Internet and networks we see today were created to connect different computers together to exchange information. By the time internet was open to public and being used widely some security related issues arise as well. When Internet was not developed security wasn’t the concern it was deemed necessary with information was being compromised. Networks are more vulnerable, furthermore all most common attacks originate from some part of networks and effect another network around the globe. Network security is one of the fastest growing fields in technology (Michael Wood, 2020). There is an ever-growing demand for development and implementation of secure networks. There are certain steps to bear in mind while designing a secure network. The first and crucial step is to follow the latest principles of secure design. Which includes identifying what we are trying to protect and from what. How to implement tools like IPS, IDS and configure a firewall. Another important point to remember is information security classification which means dividing information into groups and identify which data can be public means No risk if it is compromised and then official means low risk some personal or business information and then sensitive information which is confidential information like company records and all personal information which poses high risk if it is revealed. According to Bhaskaran There can be many techniques to design a secure network but it all depends on the organization and its needs. Network segmentation is a security measure in networks that divides the network into segments and enforces certain rules on each segment to restrict the access in case of a cyber-attack. It is safe to say that if a network designer includes all the steps while designing a network it will be very difficult for attackers to gain access and steal or compromise information. Security is all about adding more layers and make it difficult for attackers to reach the critical resources.

**Principles of secure design**

The network architecture is constantly changing and evolving over the time. That means new technologies are being invented and being used in networks to make them secure, so it is crucial to incorporate the latest security principals while designing a network. Network protections are first barrier in protecting resources from outside threats like intruders, malicious code etc. for example use of firewalls, Intrusion detection and prevention system (IDS and IPS), and content control systems like anti-virus, anti-malware, and URL filtering. A combination of Hardware and software solutions should be used. While designing a network following IT fundamental security principles should be considered.

1. Defense in depth

This approach is based on multiple layers in order to keep the network secure. According to (Wood C. 1990) better protections is achieved by adding redundant controls to protect a single asset. For example, a nuclear power plant has a fence as on outer perimeter and then combination of sensors and concrete wall to protect power plant form an invasion. If outer fence is compromised the other defenses are still active a penetration is not successful. Defensive depth can be implemented with use of single redundant security measure or combination of different measures. It all depends on the situation and how controls are placed with strong knowledge of the system. (Stawowski M. 2007) suggests that protection of IT system is based on security layers. The following rules should be considered

* Layered protection

Security layers should be associated with each other so that if one layer is by passed the other catches on to it and generate alert.

* Defense in multiple places

Security controls should be placed strategically in the IT system rather than in one place. So, the attacker does not know what he will encounter and where.

* Defense through diversification

Safeguards put in place to protect the IT system should consist of different types for example if firewall is being used, they should come from different vendors to enhance the security of the network or IT system.

The defense in depth methods should be used with cautions as adding more layers and security controls can make the system complex. Management and maintenance are also going to be difficult and costly.

1. Weakest Link

According to Cisco the system security is only as effective or efficient as its weakest link. Which unfortunately points to humans as they are often the weakest link in the chain. According to (Sasse et al. 2001) it is widely known in psychology of cyber security that users are the weakest link rather than the computer systems. The users sometime lack the judgment necessary to prevent an attack form happening and that causes the entire network breach. (Yan Z. et al. 2018) adds that Kevin Mitnick one of the famous hackers offered an insider’s view when he testified in the congress saying that “The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure devices, and its money is wasted, because none of these measures addresses the weakest link in the security”. (Standage, 2002, p. 1)

(Pfleeger S. et al 2014) The security staff should be encouraged to use simple and fundamental process to protect themselves. Company should summarize the findings in social psychology about moral values and habit formations and then combine then into guideline for the staff to transform them into better security experts. (Stawowski M. 2007) adds that when designing a network Separation of duty and job rotation should be accounted for as it limits employee’s ability to neglects and break the policy of IT system. Separation of duty states that critical tasks or commands should be executed by two or more employees. And job rotation dictates that there should be rotation between important positions of employees. Attackers most often attack the weakest link in the network and if it secure then entire system is secure and could withstand many attacks.

1. Least privileges

This security principles states that only authorized users and programs can access the resource. Privileges are set of policies that determine whether an action can be performed or not. If a user or program attempts to access the assets a request is sent to resource monitor that checks the privileges against that program or user if they are given the authority, then request will pass otherwise it will be denied and they cannot access the information or resources. (Wood C. 1990) states that least privilege is a very powerful security principle it indicates that access to information, the ability to execute and other system privileges should be restricted only designated users are given the access. According to (Schneider, F.B. 2003) Every user and program must have minimum set of permissions required in order to complete a task. It limits the damage in case of an attack or mistake it also reduces the interactions with privileged programs to avoid unnecessary use of privileges.

(Jero et al. 2021) dictates that least privilege is a significant security-design principle, but it does not protect against all threats therefore it is important to consider what threat and risks it is designed to respond. When we apply principle of least privilege or PoLP to an operating system the permissions and capabilities of the system are limited. If an attacker gain access to system process it limits his scope for example if attacker hacks into car’s head unit, he is limited to it only and cannot access the car’s steering. But there are other threat models in which system is compromised like corrupt system integrity, export data or consuming resources without providing desired output. So, it is important to place other principles to avoid the situations where PoLP is not very useful.

**Information security Classification**

Information security is an important part of network design. It is crucial to differentiate sensitive and general information. (Collared et al., 2017) defines the information security classification a traditional informatics security concept. According to (JTC, 2013) All assets should clearly be identified, and they should be owned by appointed part of the organization, Information should be classified in terms of its value and sensitivity to the organization. A set of security measures shall be placed according to organization’s classification scheme.

According to (Agrawal, C, 2007) An organization creates and stores a large amount information, and it needs to be accessed a number of employees and even other organizations. Therefore, it is important to highlight the information that needs to be protected ad what level of protection should be provided. Information security classification is based on level of sensitivity and its effect on the organization in case it is disclosed. Information security classification helps in deciding the level of security measure to protect the information. Information classification also consists of associated systems, recovery plans and operational procedures rather the just files and databases.

What classifications or title be used to identify the sensitivity of information. There are no specific rules about titles used as it depends entirely on the organization although they should clear so it’s easily understandable. Nottinghamshire County council uses three information security classifications.

* Public: This includes general information that is already known and there is no point in securing that.
* Official: This includes some degree of personal and business information
* Official-sensitive: This will include top secret information and more personal data and requires high level of security also referred to as confidential.

(Woodbury C,2007) defines Information classification as a process of determining the importance and value of information and then assigning to a category. Due to breaches and the disclosure of vital information organization across the globe realized the importance data or information thus increasingly classifying the data and taking measures to ensure the safety of information. When classifying data following rules apply

* Who can access data

Assign roles and privileges to people who can access the data and what level of access is granted to them. For example, HR managers can view phone numbers and related information of staff while accounting clerks can only view payable accounts.

* How data is secured

It defines whether data is generally available or off limits by default. Specified people have access to data, and they further have restrictions imposed. For example, some are only allowed to view the data while other can view and modify.

* Data need to be encrypted or not

It depends on the organization policies whether data needs to be encrypted or not. For example, payment card industry encrypts data as it contains very sensitive information about customers.

All these rules help in classifying information and develop company’s security policy.

**Network segmentation, IPS and firewall**

As its name suggest segmentation means divide the network into smaller chunks known as segments. This security measure focuses on splitting and dispersing the asset. According to (Wagner et al., 2016) Network segmentation partitions the network to restrict access of attacker and prevent him from gaining access to valuable resources. Different software and hardware are placed to monitor and communicate between segments.

Intrusion Prevention System or IPS is a protection measure that helps ward off intrusions. It can be a software or hardware. These products are used to continuously monitor the network and detect any attack and block the attackers (Daya B, 2013).

Firewalls is very important and recommended security measures while a designing any network that needs decent security. But as stated by (Lyu, and Lau, 2000) seeking a firewall and setting it up is not a fancy thing rather than the set of rules and policy are what make the firewall a truly secure measure. On a large-scale performance of firewall may affect the system so it is wise to choose a product that suits the company criteria.

**Conclusion**

Secure network design and development includes all the aspects discussed above. A secure and efficient network is balanced where it is easy to manage and maintain. First step is to design a secure network and implement it then constantly make if more efficient. A combination of different controls and good design can lead to a secure network able to withstand attacks and prevent any intruders to infiltrate. It is evident that threats will continue to evolve and someday bypass the security measures but so is the network security.

**References**

1. Wood, C.C., 1990. Principles of secure information systems design. *Computers & Security*, *9*(1), pp.13-24.
2. <https://www.learncisco.net/courses/iins/common-security-threats/security-architecture-design-guidelines.html>
3. Wood, M., 2020. How SASE is defining the future of network security. *Network Security*, *2020*(12), pp.6-8.
4. V. Agrawal, "A Framework for the Information Classification in ISO 27005 Standard," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017, pp. 264-269, doi: 10.1109/CSCloud.2017.13.
5. Mowery, D.C. and Simcoe, T., 2002. Is the Internet a US invention?—an economic and technological history of computer networking. *Research Policy*, *31*(8-9), pp.1369-1387.
6. Bhaskaran, A.P., Analyzing Effectiveness of Security by design Model in a Cloud application development lif ecycle which uses IAC (Infrastructure As Code).
7. Charles P. Pfleeger. 1988. *Security in computing*. Prentice-Hall, Inc., USA.
8. Stawowski, M., 2007. The principles of network security design. *ISSA Journal*, pp.29-31.
9. Wood, C.C., 1990. Principles of secure information systems design. *Computers & Security*, *9*(1), pp.13-24.
10. Yan, Z., Robertson, T., Yan, R., Park, S.Y., Bordoff, S., Chen, Q. and Sprissler, E., 2018. Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?. *Computers in Human Behavior*, *84*, pp.375-382.
11. Sasse, M.A., Brostoff, S. and Weirich, D., 2001. Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security. *BT technology journal*, *19*(3), pp.122-131.
12. Standage, T., 2002. The weakest link. *The Economist*, *365*(8296), pp.11-16.
13. Pfleeger, S.L., Sasse, M.A. and Furnham, A., 2014. From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, *11*(4), pp.489-510.
14. Schneider, F.B., 2003. Least privilege and more [computer security]. *IEEE Security & Privacy*, *1*(5), pp.55-59.
15. Jero, S., Furgala, J., Pan, R., Gadepalli, P.K., Clifford, A., Ye, B., Khazan, R., Ward, B.C., Parmer, G. and Skowyra, R., 2021, May. Practical Principle of Least Privilege for Secure Embedded Systems. In *2021 IEEE 27th Real-Time and Embedded Technology and Applications Symposium (RTAS)* (pp. 1-13). IEEE.
16. Woodbury, C., 2007. The Importance of Data Classification and Ownership. *no. C*, pp.1-4.
17. Agrawal, V., 2017, June. A framework for the information classification in ISO 27005 standard. In *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 264-269). IEEE.
18. Collard, G., Ducroquet, S., Disson, E. and Talens, G., 2017, May. A definition of information security classification in cybersecurity context. In *2017 11th International Conference on Research Challenges in Information Science (RCIS)* (pp. 77-82). IEEE
19. Joint Technical Committee ISO/IEC JTC1. Subcommittee SC 27, 2013. *Information Technology--Security Techniques--Information Security Management Systems--Requirements*. ISO/IEC.
20. Wagner, N., Şahin, C.Ş., Winterrose, M., Riordan, J., Pena, J., Hanson, D. and Streilein, W.W., 2016, December. Towards automated cyber decision support: A case study on network segmentation for security. In *2016 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1-10). IEEE.
21. Daya, B., 2013. Network security: History, importance, and future. *University of Florida Department of Electrical and Computer Engineering*, *4*.
22. Lyu, M.R. and Lau, L.K., 2000, October. Firewall security: Policies, testing and performance evaluation. In *Proceedings 24th Annual International Computer Software and Applications Conference. COMPSAC2000* (pp. 116-121). IEEE.
23. Kizza, J.M., 2005. *Computer network security* (pp. 440-455). New York: Springer.
24. Patnaik, D.P.C., Network Security: Concepts and Various Aspects for Treating the Attacks. *IJSDR2102055*.
25. Dowd, P.W. and McHenry, J.T., 1998. Network security: it's time to take it seriously. *Computer*, *31*(9), pp.24-28.