Exercise: Walling off

Introduction

Imagine you are a part of the IT team at the headquarters of Sam's Scoops located in a single office building. The organization's network is comprised of 10 office computers, 3 servers containing sensitive data, 15 employee smartphones and tablets, and 20 IoT (Internet of Things) devices, including printers, security cameras, and smart TVs. There is also a finance department with 4 additional computers that handle confidential financial information. As a new initiative to strengthen the security of the network, your task is to create a network segmentation plan.

Instructions

To complete this exercise, you will need access to Microsoft Word. If you do not have the Microsoft Word application, you can use Free Office for the web. This version of Office allows you to view and edit files in apps like Word, Excel, and PowerPoint. This free service is available to anyone with a Microsoft account.

Step 1: Understand the current network

- Before you can create a network segmentation plan, it's crucial to understand the current network. Create a list of all devices on the network, including the additional computers in the finance department.
- Identify and mark the most important devices, especially those that handle sensitive data, like servers and finance computers.

Step 2: Determine network segments

- Review your notes from Step 1 to determine network segments.
- Consider how to divide the network into separate segments to improve security.
- Pay special attention to the computers that deal with sensitive data. These may need to be placed in their own segment due to the confidential information that they handle.

Step 3: Create a network segment plan

Now that you have a clearer idea of the different network segments, create the plan.

- Develop a plan that explains how you will divide the organization's network into the chosen segments.
- Identify the segments that require firewall protection. Furthermore, provide details on how these segments interconnect with each other.
- Consider whether additional firewalls are needed to protect specific segments.

Step 4: Assess potential benefits and drawbacks

- Consider the potential benefits of your plan. Think about how your plan could enhance the performance of your organization's network and increase its security.
- Also, consider the potential drawbacks. Could your plan make the network more complicated to manage? Or could it lead to communication difficulties between devices in different segments? It is important to balance these considerations.

Step 5: Summarize your findings

- Summarize your findings in a brief report.
- Include a description of your plan, along with the potential benefits and drawbacks that you have identified.

Conclusion

Completing this exercise will provide you with a better understanding of how network segmentation can enhance the security and performance of an organization's network. You have learned to assess the current network, identify critical assets, propose segmentation, and set up security policies for each segment. In addition, you have considered the potential benefits and drawbacks of such an implementation. This hands-on experience will give you a solid foundation in planning and implementing network segmentation for any organization to improve its cybersecurity process.