

Building a Secure Home Network

Justin Rastatter jrastatter.141652@student.uwtsd.ac.uk

Introduction

This project was based on researching the fundamentals of home networking and being able to implement that research into building a secure home network, throughout this project It look at the number of threats and issues that home network face on a daily basis and how to protect your network from such attacks.

Aims and objectives

The main aim of this project was to be able to build a secure home network the objective of the report was as follows.

- To gain an understanding of security issues with current home networking.
- To understanding the multiple threats that can affect networking and how to deal with them.
- To determine what protocols to use for the home network.
- Plan a layout of the network and where to place equipment.
- Implement the information gained to plan and begin creating the home network.

Research

With this project there was a number of areas researched which can affect home networking this included DDoS attacks and the different types of DDoS attack (Botnets) ping of death floods. It also covers issues such as ransomware and how to help protect your network/devices from it. It also cover the wireless networking aspect of a home networking since most if not all home have a wireless router, it covers what you should do when getting a new router like change the default usernames and password, the pros and cons of hiding your SSID. Also why you should have a solid antivirus/antimalware on your devices.

Implementation

Taking the information from the research, the building stage of the project started, a plan was created to cover a 2 floor environment(average floors in a home), the project used the Super Hub router provided by Virgin media which was already in use before the project, since these routers aren't that great an external wireless router was used, the plan also included an extra port switch on the 2nd floor of the network, the virgin media super hub was switched to its modem mode which turns off the Wireless aspect of the router, the new router being implemented was the Asus RT-AC66U Wireless-AC1750 Gigabit Dual-Band Router.

This router has a lot more features and security settings than the standard router from the ISP and also came with a mobile app which you can use anywhere to control your network.

This app will show you whos on the network and how much bandwidth they are using, it also allows you to either block their internet access or limit their bandwidth usage.

Once the network was setup the configuration started this included changing the defaults of the new router like changing the SSID names or hiding the SSID, change the passwords to something much stronger and harder to crack.

Antivirus was also installed on all devices within the network which could use antivirus software, the one used for the project was Bull Guard this offers real-time protection, adds rules to the firewall automatically of know malicious programs and also show what sites are safe to use when browsing the internet.



References

1. D. Cameran, "Flashlight Apps Snuck Malware Into Google's Play Store, Targeting Bank Accounts
2. Norton, "What is a Botnet?," [Online]. Available: <https://uk.norton.com/internetsecurity-malware-what-is-a-botnet.html>.
3. "Cost of a DDoS Attack," Radware, 19 September 2016. [Online]. Available: <https://www.radware.com/documents/infographics/cost-of-a-ddos-attack>.
4. Cisco, "What is a DDoS Attack?," Cisco
5. N. I. Elisa Bertino, "Botnets and Internet of Things Security," *Botnets and Internet of Things Security*, vol. 50, no. 2, pp. 76-79, 2017
6. "What is a Botnet and How to Prevent Your PC from being Enslaved," Hiemdal Security, 18 February 2016

