Secure Network Design

Clive

Abstract:
In this report, I will be providing a beneficial proposal towards a network security design that will be cost-effective and much safer than the proposed setup.
The network will be covering a vast geographical range since the company is expanding by opening three more branches. Firstly, I will identify the current issues with the proposed network design by the IT technician. Secondly, I will provide examples of weaknesses and how hackers/criminals could infiltrate the existing network. As a result of this, I will be proposing a new setup which I believe will be secure and cost-effective, this solution will not only be for the present but the future as well. The new network design will also include a self-explanatory diagram as well as the benefits of the proposal as well as the limitations.
1.Keywords:

1. Firewall

2. Network

3.DDoS (Distributed denial of service)

4. FTP (File Transfer Protocol)

5. IP (Internet Protocol)

2. Critical Analysis

Vulnerability 1

The first weakness in the proposed network configuration is that there is not a backup server displayed. In modern network setups, it is almost compulsory that a backup server is implemented. The use of a backup server is beneficial for data that would be severely cost-effective should the company be unable to retrieve files.

Attack 1

The first vulnerability is different from other vulnerabilities due to it not being an attack being carried out by a hacker for example. In the case of fire, weather reasons or even the case of theft the data would then be permanently lost and to regain such data would heavily cost-effective in terms of time and cash, as explained in [5].

Vulnerability 2

In the second vulnerability, the company is using an FTP server. This server is responsible for file transfers across the company, a point to mention is when a request to log into is made the user machine send across their username and password in plain text as a result of this the login information can be retrieved.

Attack 2

Due to the fact, the data is not encrypted this can be retrieved through the use of Packet Sniffer such as Wireshark. With this software ‘Packet Capture' can be attempted as mentioned in [1]. A Packet Sniffer would capture packets sent across the network. Once the data packets have been captured they can be decoded through free online tools available to anyone as a result of these tools data can be obtained.

Vulnerability 3

Thirdly, another weakness in the setup is that IP packets are being sent over the internet without having any security implemented. If there is not any security on the packets, then there is no origin authentication of the sender of the packets. If the system is not able to confirm the sender of the packets, then is a highly invalid procedure for a network to be running. As the company

is going towards a WLAN IP is not secure enough to confirm who the users who are sending data across the network.

Attack 3
This is severely dangerous because the packets could be transferred from a hacker impersonating an employee. The unauthorized user could use IP Spoofing to send packets across the network as there is no origin authentication implemented in the current system.

Vulnerability 4
The fourth weakness as exposed in the current configuration is the use of the Packet Filtering Firewall this shouldn't be approved for something like a bank for example as it is much less secure when you make comparisons to other Firewalls available in the market.

Attack 4
Just like the previous attack with this type of Firewall being used IP spoofing attacks are possible. Additionally, the firewall cannot prevent an attack based due to an application-based vulnerability this is the result of how the firewall only works in the Transport and network layer as explained in [2].

Vulnerability 5
The fifth weakness in the network configuration is that the DNS (Domain Name Server) is set up with default settings. Since the setup is at the default state it does not use the latest software available to DNS also it lacks fundamental security.

Attack 5
Due to this vulnerability, an attack known as DNS cache poisoning also known as DNS spoofing can be attempted by a criminal. The goal of this is to divert traffic in terms of IP packets from company servers to unauthorized servers. A major security fear is that once a DNS server is poisoned, then it can spread to other DNS servers for the same company.

3. Secure network design proposal

Solution for vulnerability 1
To get a solution for this vulnerability of not having a Backup Server implemented or suggested, I would, therefore have a server which is responsible for storing backup copies of data. Unlike the other servers, I would keep this server offsite. This is mainly in case of the threats of data as mentioned in the first vulnerability, if they were to be successful, then the company wouldn't be affected for a long period and could commence working as usual since there is a copy of the data stored offsite.

Solution for vulnerability 2
To resolve the issue specified by using an unsecure method of transferring files, I would recommend, using SFTP (SSH File Transfer Protocol) over FTPS and FTP. The reason is that it provides a secure encrypted connection compared to the originally suggested protocol(FTP). However, compared to FTPS which is based upon SSL, it is much easier to implement. For example, for a user to establish a connection to the network, they will require a username and password, but with an FTPS the user makes the same requests but also a certificate this method needs more time to be implemented also it requires more storage to keep the certificates stored.

Solution for vulnerability 3
To resolve this vulnerability, I would recommend integrating IPsec into the network layer, due to the benefits explained in [6]. This is so the IP would, therefore have more security as you would be able to verify the sources of where the IP packets come from. Also, it can prevent attacks such as replay of old packets as well as DoS attacks. Additionally, to get a

Virtual Private Network operational for staff members to be able to access files from an external location, I would consider implementing IPsec with tunnel mode. The benefit of using Tunnel Mode is it will protect packets coming outside of the host (outside of the company). Also, I would suggest providing an additional protocol for Encapsulating Security Payload(ESP). It requires more cost when you compare it Authentication Header however it protects the TCP packets also it provides encryption on the TCP ports additionally the security though ESP is better as a result of the traffic being hidden, hence providing Data Integrity.

Solution for vulnerability 4
To resolve this vulnerability, I would recommend implementing a Circuit-level Gateway to replace the current packet filtering firewall. This choice was difficult due to the Application-level Gateway being acceptable to overcome this current vulnerability, however, Circuit-level Gateway provides a lower cost as well as better overall performance. Due to the fact that the preferred solution distributes TCP segments without examining the contents which will provide confidentiality of data.

Solution for vulnerability 5
To prevent the issue of having a default configuration on the DNS Servers, the company will need to ensure that the latest version of DNS is installed across the DNS servers. Also, they will need to a piece of software known as BIND one of the beneficial feature that BIND provides the random use of ports associated to the DNS this makes it much harder for DNS poisoning attack to take place. Additionally, the software encrypts transactions IDs. Finally, the IT department technicians will need to ensure that the only services on the DNS server are ones which are required this is because any extra services on the servers will only increase the chances of a successful attack.

Additional Requirements

Authentication
To provide authentication for the network setup, I would recommend for the company to use the Kerberos authentication protocol this would be implemented throughout all services in the company for example when a user logs in. The advantage of having authentication like Kerberos is that it will also authentication a user when they are using a non-secure network (external access). One significant advantage of using Kerberos is that it generates temporary keys also known as session keys also all keys are encrypted through secret key cryptography. I would deploy Kerberos on a standalone server with single realm installation, this decision was due to comparing the overheads and cost of implementing Kerberos on a cross realm. Also, another drawback of having a cross realm server is that you require two servers, so if you need to diagnose a fault on the system then you need to find out which server has the fault.

Access control
Access control is required for users to comply with company procedures when it comes to the use of files without breaching any security. As a result of this being quite important, I will be suggesting the RBAC (Role Based Access Control) Model. I have chosen this because it works on an employee role within the company. The person in charge of organising the roles and access within the company would be done by the Network Admin. This is useful because if everyone were able to do anything in the company, then there wouldn't be a need for a hierarchy in the workplace also there would be more chance for crimes like fraud to occur.

Remote Access
To be able to securely access files when you are out the office can be useful as the company wants the employees to have that capability. As mentioned in my third solution I would suggest having a VPN because it ensures the connection is secured and cannot be monitored

from an external source this is useful when employees are trying to access confidential files externally as explained in [7].

Solution to DDOS Attack

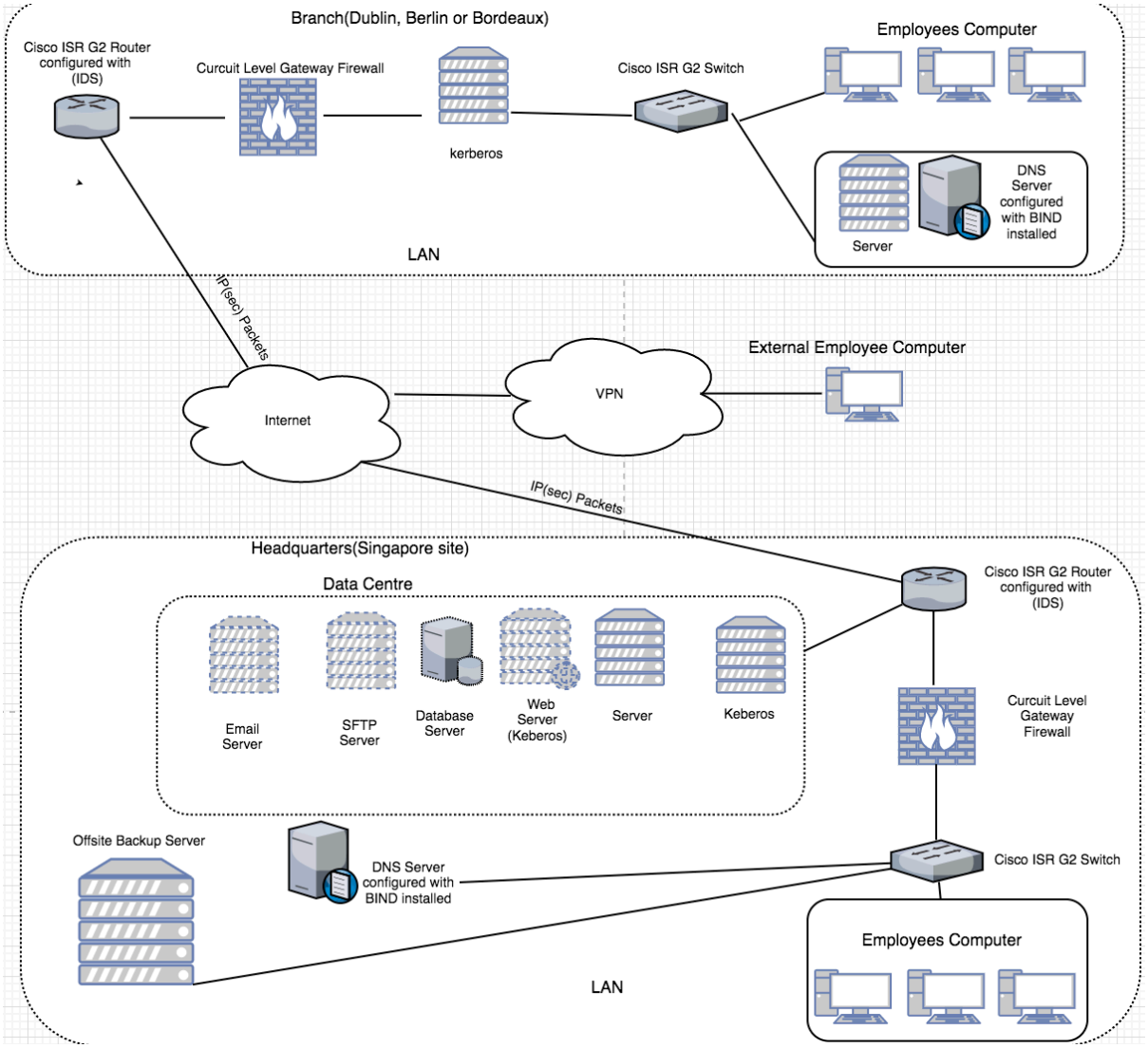
I would recommend upgrading the routers and switches to the 'Cisco ISR G2 series' as a solution recommended from CISCO themselves for business which revolved around banking. When these are configured they will then provide successful security as well as being used by the business for the foreseeable future. The configuration will provide will include (Intrusion Detection System) IDS this is so we can prevent these types of attacks while they are in operation. With the use of IDS, I will be using the Anomaly Detection this is because the database of this system requires updating although some people may argue that this is not ideal, the methods that hackers will use will constantly change so this type of Detection will be able to recognize types of attacks which are unknown to the system. Additionally, I will be distributing the IDS on the routers, so this will be a Network-based IDS as I find it beneficial to the system to be able to monitor lots of network traffic.

Cost-Effective

I believe my network proposal is cost-effective I have managed to provide one solution to solve more than one issue such as my third solution due to this it can also provide the tools in order, for remote access to be installed, which is a useful feature. Additionally, I have suggested a backup server due to it being standard practice, but if the company were to lose several millions of customer records, for example, it would be much costlier to re-obtain the data than having a backup server.

Also, I have used free software as stated in [3] & [8], to be implemented on the DNS server and the Kerberos Server in this case.

4. Diagram



5. Conclusion

The first design which was proposed from the IT technician. Had numerous security issues, especially the fact that it hasn't even covered the basics such as having a backup server and not using any security features. The backup server is vital because the whole point of security on a network is to not make a network impossible to be attacked but in fact it is judge on how well, it can prevent an attack and how fast it can recover if the company was attacked from hacker(s) or other variables.

With my proposal I believe it can prevent attacks that I have explained in this report but also, I have supplied the additional requirements. However, I do think the drawbacks of my proposal that it will need constant maintenance for things like the IDS and the Access Control, but I think with constant maintenance being done on the network then it can be possible to keep it update to date and with this the network design can last for some considerable time.

References –

Reference number 1
Security risks of FTP and benefits
https://thehackernews.com/2013/12/security-risks-of-ftp-and-benefits-of.html

Reference number 2
Introduction to Firewalls
http://etutorials.org/Networking/Router+firewall+security/Part+I+Security+Overview+and+Firewalls/Chapter+2.+Introduction+to+Firewalls/Firewall+Categories/

Reference number 3
Berkeley Internet Name Domain
https://www.webopedia.com/TERM/B/Berkeley_Internet_Name_Domain.html

Reference number 4
Financial Banking Solutions
https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Financial_Services/Financial_Branch_Banking/financial_banking.pdf

Reference number 5
Cost of Data Loss
https://blog.netapp.com/blogs/calculating-the-cost-of-data-loss/

Reference number 6
Understanding IPsec
https://www.simplilearn.com/understanding-ipsec-rar37-article

Reference number 7
Why you should start using VPN
http://www.lifehacker.co.uk/2012/09/05/start-using-vpn-choose-best-one-needs

Reference number 8
Kerberos
http://web.mit.edu/kerberos/