Designertech Company and Security Threats

Small companies are more likely of being victims of data leaking and net attacks. Designertech is a group that has had a big growth, and through the years they have experimented some threats, in this document it is going to be analyzed some of those:

Malware

This security threat is directed by viruses and worms which are developed by cyber attackers, in order to obtain access or cause damage to the company network or on its devices. The fast developing of malware is a great concern for companies as Designertech, in just a few months a company might catch around 2000 segments of virus per day, occasioning system slowness, interruptions on the internet and incapacity for accessing files and data. (Grishko, 2017)

Data Loss

Revealing information or getting affected by a computer crime, it would be one of the most dangerous threats for a company such a Designertech that handles critical information which has been the reason of its success. If the corporate secrets get revealed, this might mean not just the loss of money, it would mean exposing the formula of its success through its operations, intellectual goods, and contact details of the customers, partners and confidential data. (Grishko, 2017)

DDoS Attacks

The goal of this attack is to attempt to get a service unavailable by generating a big amount of requests or traffic from multiple sources. Since Designertech manages multiple services, this threat could mean a risk for the continuity of its operation. Currently one of the disadvantages for the company is the lack of an SSL certificate on its website, making it insecure and vulnerable to this type of attacks. (Digital Attack Map, 2013)

In addition, address task 3 in page.

Information Security Policy

The creation of the security policy for Designertech is approached to some important aspects

such a VPN policy, password policy, server security policy, information sensitivity policy, anti-virus guidelines and risk assessment policy. The security policy was provided by Designertech and it will be attached as an informative annex.

Traditional or Building Block Network Design

The chosen model for the company was the building block network design. This model allows Designertech to organize the services in diverse categories subject to the customer necessities. The design outlines all the corporate resources such as server farms, VoIP and internet access in blocks over WAN connections. Even though Designertech is a small company and does not have more connections with other headquarters, its internet channel and the connection with its services provider is indeed important for the correct operation of the business. Designertech has the main firewall which connects 3 different plants: Sales/Finances area, Operations/ Support area and server farm area. Also, it has a connection with its service provider through a WAN router, which together with the firewall allows the remote access to the internal net through the VPN.

Analysis of the Requirements

The company has physical facilities located on Great South Rd, Penrose in Auckland. The building is composed of 3 plants: One for sales/finance area, second for operations area and the last one is the servers area. Each department has its own communication zone with approximately 20 computers and 20 telephones for each plant, besides 3 servers located next to the operations area. All these devices are connected to 3 different switches which in turn are connected to 1 firewall and this last is connected to the WAN router that is in charge of allowing the connection with the service provider. Employees of Designertech must have a connection with the internal net, in case of required remote access. On the Firewall is created all the policies to allow and deny the traffic and different users permissions, besides protecting the internal network from intrusion.

Technology Design

WAN Security

The Designertech security net is founded on the IPsec protocol which provides information confidentiality by means of a robust encryption, data integrity and permits implement a VPN over the internet channel. (Cisco, 2018)

IPsec VPN has converted the most common method to guard company's traffic over the

internet. The followings are some features of the VPN design for Designertech:

It was configured a fixed IP for the connection to the VPN.
It was used a digital certificate for the authentication in the VPN. This provides a high level of security and an easier way to manage the credentials and passwords.

Defending the Perimeter

Designertech makes used of a Firewall which is providing a strong security and control from the traffic that flows through the network. The main function of the Firewall is to create limits between all the internal network segments. Via ACLs, the FW provides strict control of the traffic, and it creates politics to allow or deny the access. (Cisco, 2018)

The FW at the same time is providing an intrusion detection system which is acting as an intrusion detector sensor, looking after packets and sessions flowing in the network in order to detect suspicious activities and reacts before the network security can be compromised. The 3 main actions the system does are: To send alarms to the management interface, to drop packets in case of being suspicious and to reset the connections. (Cisco, 2018)