Regional Insurance Group Current Network Report

The current network infrastructure of Regional Insurance Group supports both internal business operations as well as customer access. The network provides internet connectivity, internal communication between the different systems, and access to the critical services of the business such as customer management, database storage, and file sharing. The network is protected by a single perimeter firewall and relies on a single managed switch, using IPv4 addressing to connect internal devices.

The company hosts a public facing web server that allows customers to access the company's online portal. This server is operated using a linux system and an apache web server platform. This server has also been placed in a demilitarized zone or a DMZ. This provides controlled external access from the internet. The DMZ separates publicly accessible services from the internal corporate network to reduce the risk of unauthorized access to the sensitive data held within the internal systems.

Behind the firewall, the internal network supports several different servers that provide different services for the company. Two servers each are assigned to customer management, database storage and file storage. The customer management systems process requests from internal workstations and communicate with the database systems to retrieve and also store information.

The windows database servers are responsible for storing sensitive customer information and organizational data. The last two servers, the file and print servers provide file storage and print capabilities for employees throughout the organization.

The last component of the network includes 50 windows workstations for employee access which are also connected to the internet through the managed switch. The switch serves as the main connectivity point that links all the workstations and servers within the local area network. The switch manages the traffic flow between all of the devices and ensures reliable communication using IPv4 network addressing.

All the systems are connected through a hierarchical structure where the firewall serves as the entry point between the internet and the internal systems. The firewall filters incoming and outgoing traffic, according to its configured rules, which helps to prevent unauthorized access to internal systems. From the firewall traffic is routed to either the DMZ web server or to the internal network through the managed switch infrastructure.

Although the network does support the essential services and connectivity, the current setup presents potential security limitations. The organization relies on a single border firewall for protection and it lacks deeper internal segmentation between the critical systems. As a result, if an attacker were to gain access to the internal network. Sensitive systems would be reached quite easily. Improving segmentation and implementing additional security controls would greatly strengthen the overall network security.