Sarah Barettino
1301 Club Ave
Allentown, PA 18109
570-801-1817

10/31/2023

Chris Nelson
President
Greenfield Properties
123 Sophia Way
Minneapolis, MN 55000

Dear Mr. Nelson:

I am grateful for the opportunity to offer my expertise in network planning guidance for the Greenfield Properties project. The merging of Bluegrass Rentals and Redstone Property Management has allowed for many new technologies and techniques to be applied and considered as you grow your new company.

After careful review of current assets and your requirements I have compiled my recommendations to optimize your network baseline. My recommendations includes ideal network architecture, organization, and security protocols to serve as a foundational blueprint.

Enclosed you will find those recommendations. Please reach out if any further clarification or changes in requirements are needed and I would be happy to reevaluate my recommendations.

Sincerely,

Sarah Barettino

Introduction

The IT recommendations for Network Structure and Security for the merger of Bluegrass Rentals and Redstone Property Management into Greenfield Properties.

Network Infrastructure

Current Employees – 46 – 1 remote

Total Device – 95

- **PC –** 26 – 1 remote
- **Tablet –** 30
- **Smartphone –** 39 – 1 remote

Based on the following information a **client/server** architecture is ideal. The majority of the employees work on-site so a **LAN** set up would be ideal, LAN provide excellent speed and low latency which will be ideal for your current needs. **CAT6** will be used throughout, Phelum rated cables used when running though ceiling terminating in a designated secure network closet. In addition to a network closet, a secure server room will also be required. The benefit of a client/server architecture is ability to share resources efficiently. The following servers are recommended to meet your requirements.

- **File Server –** Allow for multiple hosts to access and update business files. Security and permissions can be added to provide additional layers of protection.
- **Application Server –** *Cloud* **-** As per your requirements, you have a proprietary application that all employees need to access. This server would allow for secure isolated access to the application.
- **Print Server –** The Print Server will allow for seamless printer resource sharing. Once established the Print Server will be easy to scale and manage the printer resources in the most efficient way.
- **Database Server –** *Cloud* **–** Centralized location for data that can be linked, queried and updated remotely.
- **Active Directory Server –** Manage user profiles, permissions, roles, access and availability in a central location.
- **Web Server –** *Cloud* - Public server that would store your public website. I would recommend separating your proprietary employee application and your public website.
- **Mail Server –** Listed requirements did not mention whether you were contracting with a third party provider. If not a Mail Server would be recommended.

I am recommending a **Hybrid** cloud environment based on current needs. Hybrid will allow you to be able to utilize the Cloud Service Providers expertise in security for specific resources that are high risk targets. Additionally, many cloud providers offer varying options of cost, scale, control and responsibility sharing so depending on whether you have the expertise to manage resources and assets in house or whether you need a managed service can be decided on a

case-by-case basis. Cloud especially for databases provide an extensive back up standard that will also be extremely beneficial.

Operating System Recommendations for Assets

Windows – Windows Server Standard

- **Client PCs –** Most employees are trained on Windows use and capabilities
- **File Server –** Windows offers extensive sharing capabilities and is compatible with Windows clients.
- **Print Server –** Windows again for ease of compatibility
- **Active Directory Server –** Standard choice seamless management when managing Windows clients

Linux - Ubuntu

- **Application Server –** Linux because it is extremely stable, secure and cost effective
- **Database Server –** Linux – I would recommend utilizing a managed service through CSP
- **Web Server –** Linux because of the stability

I recommend Windows Server Standard and Ubuntu Server for the distribution options. Windows Standard currently would be sufficient in your current state to meet all your needs, when you scale up this will have to be revisited. I would run Linux on the public virtual servers as it is most cost efficient and secure option when dealing with public servers.

Network Segmentation and Printing

Dividing networks into smaller segments can help with troubleshooting, security and enhance network performance. Less network load because broadcast segments are smaller. I would start by grouping based on department and authorization status, this can ease resource management and make maintaining least privilege management easier.

Total of 8 Subnets

Corp LAN	Executives Office Manager HR Reception	9 hosts	/28
IT LAN	IT	2 hosts	/30
Marketing	Advertising Public Relations Social Media	2 hosts	/30
Sales	Leasing Manager Leasing Agent Leasing Assistance	13 hosts	/28
Property	Property Owner Liaison Property Manager Maintenance Manager Maintenance Specialist	16 hosts	/27
Finance	Accountant Accountant Specialist	4 hosts	/29
Private Resources	Database File Server Print Server Application Server	4 hosts	/29
Public Resources	Web Server	1 host	/30

I would also recommend utilization of a VLAN. VLANs offer more control and adaptability. VLANs can add more information for addressing issues and troubleshooting. Using a VLAN in conjunction with a subnet structure will increase security and scalability.

Printing

Print Server

PROS	CONS
Load Balancing User Authentication Queue Management Centralized Management Scalable	Single point of failure Difficult to configure

IP Printing

PROS	CONS
Simple No Single Point of Failure Cheaper	Limited control Driver Management Lack of User Authentication

I would recommend a Print Server for your company because Greenfield is too large and complex for IP Printing. Your emphasis on security is also a factor. Considering that the company is already planning increasing scale being proactive and preparing the environment

now will enable the IT department to work out any issues they may have while the scale is still small.

Wi-Fi Networking

Depending on the building structural composition we can assume that both tablets and smartphones will need to connect to the network via Wireless Access Points when in the building. Current wireless asset count is 68, 30 Tablets and 38 Smartphones, with a 50% planned increase during future expansion would bring us to 102 devices needing connectivity.

We will need to run CAT6 cabling in the phelum space from our current switch structure to 12 Wireless Access Points mounted to the ceiling.

Each on the WAP devices will be spaced approximately 50-75 ft from each other. All will be assigned the same SSID but be designated one channel of 1,6, or 11 so that there is continuous coverage without having to change networks.

A wireless LAN controller will be utilized to streamline the coverage, configuration and management. All WAPs will be set to WPA3 encryption. As will be discussed in a later section an extensive policy for Acceptable Use, and Security policies will need to work in conjunction to ensure that the wireless network traffic is limited to low security items and high security items need to be run through the LAN PC computers.

Security Measures

Greenfield Properties has data that needs multiple layers of security. The first layer of security and the most important is employee awareness and training. I highly recommend multiple planned security review meeting throughout the year in addition to all the security measure that will be in place.

Physical Security

All IT equipment will be stored and secured in one zone of the building. I would recommend one room that within contains an additional secure area for the on-site servers and is monitored with motion activated CCTV that can be reviewed if a breach is discovered. The interior server area should be accessible only with a key and RFID badge. Outside the secure server area is where the switch and router closet. This door will be accessible by a RFID badge.

Infrastructure Access

In addition to the physical securing of the infrastructure I would also recommend some logical protections to be utilized. On such important and efficient is port managing.

I recommend closing all ports except those specifically needed for the host. An example is on the file server shutting all incoming ports except SFTP request so port 22 will limit how many ports can be accessed and used for a malicious attack. It is an easy thing to configure that provides a multitude of protection.

Authentication

Using the Kerberos method will enable the user to only have to log in once to establish their identity and then they will have access to the resources they have privileges for. This will limit the need for multiple passwords and will also increase password security because they only have the one to remember.

Lockout Policy

Lockout policy will be a full lockdown after 5 attempts. IT will need to be contacted to reset password after identification verification.

Password Complexity Requirements

Requiring 8-15 characters at least one upper, one lower and one special character, password change every 45 days. This is the best practice for establishing a strong password.

Firewall

Network Firewall with a UTM – to protect the private network from the public, it is the first line of defense for the entire network.

In addition to the Network Firewall, I would also recommend IDS and IPS on the resource subnet where the database would reside.

Anti-Malware

Cloud based anti-malware for resources in the cloud because CSP provide the most up to date security for online attacks.

Utilizing Host Based Anti-Malware and Heuristic scanning for onsite hosts and resources. Host based Anti- Malware can schedule regular interval scans, schedule regular virus dictionary updates and engine will also insure we have the most up to date profiles.