VIP Events Cybersecurity Prosposal

VIP Events is a small catering and food equipment leasing company operating out of a single building and various storage containers. The company has received a capital investment and is preparing to move to a new premises. This is a major step and requires a well thought out plan. The company is looking for solutions to address these needs and challenges related to the security.

Scope: The scope of the proposal is to crearte a well-structured security network architecture. The aim of the proposal is to guide VIP Events to help them achieve their goal of setting up the new infrastructure with Azure AD. With security as the main consideration, the goal will be to incorporate various security priniciples at each step of the process so that VIP Events poses strong security posture and complying the required law.

Building Structure and Network Design

Building Structure: VIP Events' new building consists of three floors.

- The ground floor of the building houses all the culinary equipment that the company lends. It also has a loading dock for the equipment.
- The first floor of the building consists of the kitchen and storage for the food preparation.
- The second floor of the building is used as a office space where all the administration related work is conducted.

Network design:

- The company should employ Azure Virtual Netwrok feature of the Azure AD
- The network for the company should be segmented into three different subnets.
- The subnets can be named bassed on the each level of the building i.e., the subnet for the ground floor can be VIP Ground, VIP Kitchen for the first floor and VIP Office for the second floor.
- The purpose subnetting is to limit the access to resources each department has and adds extra layer of defense.

- By segregating the network the company can isolate the network and devices that are affected in case of a cyberattack. It also prevents lateral movement.

Wireless network configuration

VIP Events can benefit a lot by employing Azure Virtual Network in the Azure AD. This offers various benefits.

- It allows company to connect its resources to the internet.
- It also allow the company to divide the the network into various subnets
- Each subnet can be configured to use secure protocols like HTTPS while connecting to the network

VIP Ground Subnet:

VIP Ground Subnet device allow list			
Devices	**Equipment Manger**	**Equipment Handler**	**Temp Workers**
Desktops	1	NA	NA
Laptops	NA	NA	NA
Tablets	1	4	NA
Mobiles	1	NA	30 (RBAC)

- This subnet should be configured to only allow devices used at the Ground floor to be connected
- This subnet should mostly be used to access equipment management function of the app
- This subnet should also allow the temp workers to perform day to day operations with restricted access

VIP Kitchen Subnet:

VIP Kitchen Subnet device allow list			
Devices	**Catering Manger**	**Head Chef**	**Chefs**
Desktops	1	1	NA
Laptops	NA	NA	3

Tablets	1	1	3
Mobiles	1	NA	NA

- This subnet should be configured to only allow devices used at the Kitchen floor to be connected
- This subnet should allow the devices to access Kitchen management function of the app

VIP Office Subnet:

VIP Office Subnet device allow list		
Devices	**CEO**	**Office Workers**
Desktops	1	3
Laptops	NA	NA
Tablets	1	NA
Mobiles	1	NA

- This subnet should be configured to only allow devices used at the Office floor to be connected
- This subnet will involve most of the administration work and event management.

Access control and security policies

VIP Ground Subnet:

- The devices allowed at this subnet are tablets used by equipment handlers and the desktop used by the equipment manager
- The operational access to these devices will be granted via assigned Azure AD usernames and strong passwords and implementing MFA
- The users in this subnet will be assigned to Network Security group named Ground_NSG
- The Equipment Manager will be in charge of regulating access to the equipment, conducting inventory counts, conducting audits and assigning day to dayu operations for the temp workers

VIP Kitchen Subnet:

- The devices allowed at this subnet are devices used by the catering manager
- It will also include desktop and tablet used by the Head Chef
- It will also include tablets and laptops used by chefs

- The operational access to these devices will be granted via assigned Azure AD usernames and strong passwords and implementing MFA
- The users in this subnet will be assigned to Network Security group named Kitchen_NSG
- The Catering manager will regulate the access at this level of the network for the Head chef and other chefs

VIP Office Subnet:

- The devices allowed at this subnet are desktop, tablet and mobile phone used by the CEO
- It will also include devices used by the office workers
- The operational access to these devices will be granted via assigned Azure AD usernames and strong passwords and implementing MFA
- Moreover the access is also regulated with PIM and JIT Access
- The users in this subnet will be assigned to Network Security group named Office_NSG
- The CEO will have access to all the resources of the company

User roles and access requirements

1. **CEO:** The CEO role of the company will have unrestricted access to all the functionalities of the app.
    a. Will be assigned the Global Administrator Role
    b. CEO will have a designated username and will have to follow a strong password policy for the account that contains uppercase and lowercase letters, numbers and special characters.
    c. The password will have to be at minimum of 12 characters
    d. The CEO role will also have to authenticate itself by MFA
    e. The CEO user account can only be accessed from the registered devices
2. **Office workers:** The office workers will be responsible for data management and office work such as making appointments etc.
    a. Require username and password to access resources
    b. MFA required
    c. Will be a part of Second_NSG
    d. Account access only from registered devices
3. **Catering manager:** The catering manager will have the access to the event management functionality of the app and will be responsible for the planning and managing events, menu planning and logistic management.
    a. Will require a username and password to access the resources
    b. MFA required
    c. Will be the administrator for Second_NSG
4. **Head Chef:** The head chef will be responsible for overseeing kitchen management and will require elevated access to the kitchen resources
    a. Will require username and password

   b. MFA required for the access to resources
   c. Will be responsible for ordering supplies for the kitchen
   d. Regulate access for the chefs
   e. Will be the administrator for First_NSG
   f. Restricted to first floor resources
   g. JIT access to certain resources
5. **Chefs:** The chefs will be responsible for food preparation and kitchen management.
   a. Will require username and password to use resources
   b. MFA required
   c. Will be a part of First_NSG
   d. Physical access to the kitchen
   e. Restricted to first floor resources
6. **Equipment Manager:** The equipment manager will be responsible for management of all the equipment and will have elevated access to Equipment management function of the app.
   a. Will require username and password to use resources
   b. MFA required
   c. Will be the administrator for Ground_NSG
   d. User account can only be accessed from registered accounts
   e. Regulate access controls for the equipment handlers
7. **Equipment Handlers:** This role will be responsible for tracking and handling culinary equipment.
   a. Will require username and password to use resources
   b. MFA required
   c. Will be a part of the Ground_NSG
   d. Restricted to ground floor resources
8. **Temp Role:** This role will be assigned to temporary workers who will be responsible for the day to day operations.
   a. Will be assigned temporary usernames and passwords
   b. Require JIT access
   c. Needs approval from the Equipment Manager
   d. Restricted access to the resources

Roles	Access to Second Floor Resources	Acces to First Floor Resources	Access to Ground Floor Resources	Restriction type
CEO	✅	✅	✅	Unrestrictive
Office workers	✅	❌	❌	Restricted
Cartering Manager	❎ (JIT Access)	✅	❌	Restricted

Head Chef	❌	✅	❎ (JIT Access)	Restricted
Chefs	❌	✅	❌	Restricted
Equipment Manager	❌	❎ (JIT Access)	✅	Restricted
Equipment handlers	❌	❌	✅	Restricted
Temp Workers	❌	❌	❎ (JIT Access)	Restricted

Physical security guidelines

- The physical access to the premises should be restricted or secured using security guards and use of locks
- The staff at ground level should be restricted from having acces to first level resources
- The equipment manager should restrict the physical access to the equipment used by the staff i.e., tablets and desktop used at the ground floor.
- Access keys should be put to use access each level's resources
- Each key should be properly authorized

Setting up Azure AD tenant

In order to incorporate the company infrastructure to the Azure AD, the company will need an Azure AD tenant and have to choose to a subscription. To do this the company need to create a Microsoft Entra ID account and choose the specific plan that suits the company.The company will benefit from the P2 edition subscription of Azure AD which is the highest tier.

Following are some of the steps to set up the infrastructure:

- The company needs to set up required VMs for various purposes i.e., hosting apps and databases
- Set up Microsoft Intune to register company devices to be used for cloud service
- Set up Azure AD connect to migrate and syncornize existing AD resources to the cloud and the company can also chose to set up Azure AD Coonect health to monitor and report the health of syncorniztion process
- Create user accounts and assign group based controls

User account configuration

After setting up an Azure AD tenant and appropriate subscription, user acoounts should be configured.

- It involves creating user accounts and strong passwords
- Implementing MFA
- Implementing password policies to enforce adoption of strong passwords
- Assigning appropriate attributes
- Creating security groups
- The company can configure SSO for the users as well so they don't have to enter the passwords over and over to access different Azure resources

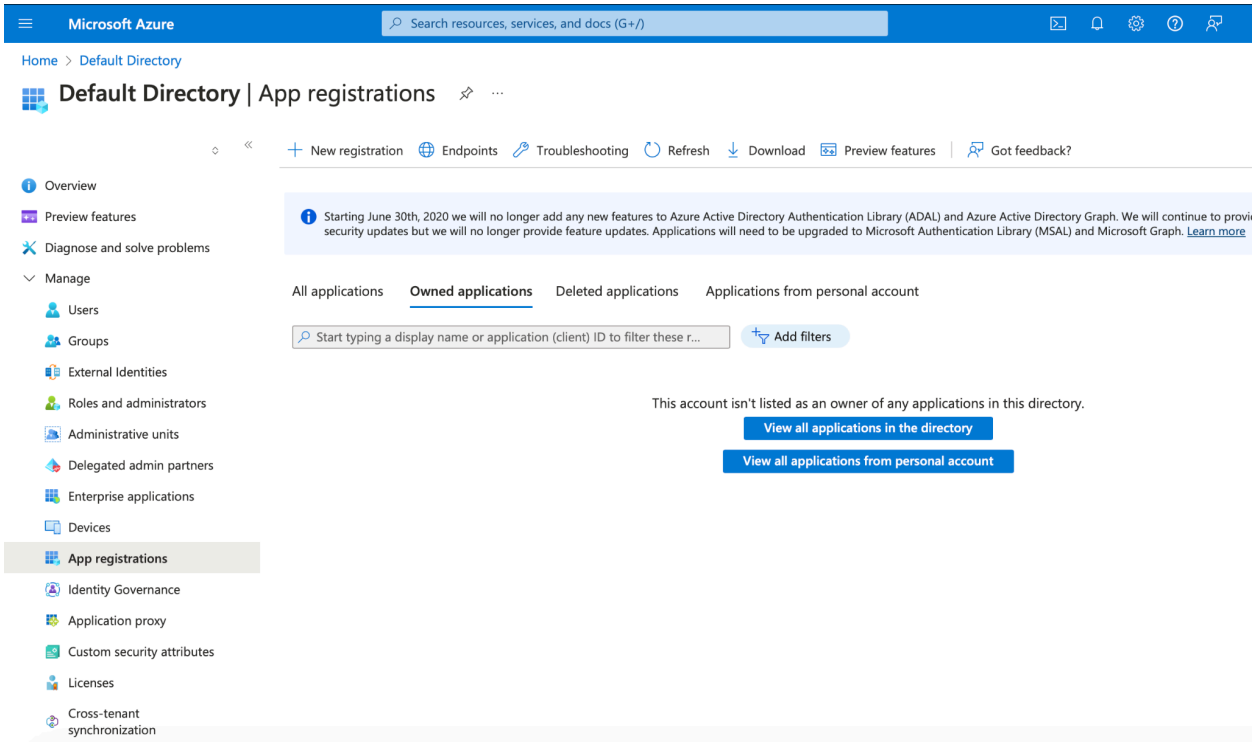
Group-based access control implementation

The company should also implement group-based access controls. Implementing group-based access controls will allow the company to implement policies to the entire group rather than doing it individually to each user

- Resource Group feature Azure AD will help addressing this need
- This option will allow the company to assign employees with similar roles in one group
- By assigning resource group the company can implement policies at group level
- Resources like Azure VMs can be assigned so that only certain groups can use that resource
- It will also help with more granular control

VIP Food app integration

In order to integrate the VIP Food app with Azure AD, the company will need to register it under the Registration an application option in Entra ID menu.



Custom Azure roles

The company will need to employ custom Azure roles feature of Microsoft Entra ID P2 tier. This feature will allow the company to define role permissions. Customized roles allow granular control over the resources. The company can create a custom rule for the application that allows the user to make changes to certain features or use certain features. For example, equipment management will need more control over the equipment tracking and coordination feature of the app whereas equipment handlers might only require bare minimum access to the app feature.

- Administer Role
- Manager Role
- Employee Role

Assigning permissions to Azure roles

Next the company will have to assign the permissions for the custom roles. The permissions can vary from read, write, action and delete.

1. **Administor Role**:
    a. Will have the most control of any roles
    b. Will have the permission to Write/Action/Read/Delete

2. **Office Role:**
    a. Will have Write/Action/Delete
3. **Manager Role**:
    a. Will have some high level permissions like Action/Read/Delete
4. **Employee Role**:
    a. Will have only action/read permission
5. **Temp Role:**
    a. Will have only read permission

Mapping user groups to Azure roles

Roles	Custom Roles
CEO	Administrator Role
Catering Manager	Manager Role
Equipment Manager	Manager Role
Office Workers	Office Role
Head Chef	Manager Role
Chefs	Employee Role
Equipment Handlers	Employee Role
Temporary workers	Temp Role

Client app integration

The company can check if the client app has been integrated into Azure AD properly using Azure AD Connect Health. Furthermore, the company can also use user credentials with different role assignments to log in and try using apps and its different features.

User account validation

The user account validation can be performed in various ways. One way the company can check validation of user account is to try logging in to Azure AD with the credentials of an user account. If the user accounts are migrated from an Active Directory using Azure AD Connect, then company can employ Azure AD Federation service so that user will be able to use the same credentials as AD to log in to Azure AD resources. Moreover, the company can use Azure AD Connect Health to check if the synchorinization between AD and Azure AD is healthy or to see if there any errors during synchornization.

Application role assignment

The company will be able to check the application role assignment by checking App Roles option under App registration menu. In order to perform testing of app functionality based on application role assignment, the company will need to log in to Entra ID using one of the user's account with an application role assignment.

Group/Role-based access testing

The company can conduct Group/Role-based acces testing by logging in to Entra Id using credentials of user with Role-based access. The goal of this testing is to see if the level of access user have to certain resources. If user's credentials allow you to access resources that shouldn't be accessed by that role then the company needs to reconfigure the Group/Role-based access and see where the mistake was made. The other way of testing Group/role-based access is to check the Group/Role permissions assigned to a user.

MFA verification

MFA verification for users can be validated using a conditional access policy for a Group or a User. To check if the MFA has been implemented for a certain user, you can either try using user credentials to log in or you can check if the MFA option has been ticked in Conditional Access Policy for the certain group. The company also needs to make sure that what resources require MFA. For instance, it could be the company's application.

Logging and monitoring

Azure monitor will help company monitor all the resources in Azure AD. The company can leverage Azure monitor and Log Analytics to see any irregular activities such as failed log in attempts. To check changes to role assignments and user attributes the company can use Activity log feature.

User authentication policy

The company should strong authentication policy using Azure Policy feature of Azure AD. This feature allows you to define the conditions required for a certain role and resource. For example, you can create a policy that enforces user to have a password that contains atleast 8 Alphanumeric characters and special symbols. The company can also implement a policy that

enforces use of MFA while granting access to certain critical resources. Azure policy allows you to create custom definitions for a tailored experience.

Network configuration policy for web applications

The company should create a new policy for network configuration for its web app. Azure Policy has built-in definitions that can help VIP Events secure its web app. For example, Azure Policy has “All Internet traffic should be routed via your deployed Azure Firewall” built-in definition that routes all the traffic from web app to the Azure firewall to detect illegitimate requests. Some other examples include “Configure network security groups to enable traffic analytics”, “App Service apps should use a virtual network service endpoint” etc. The company should leverage this feature to secure its web app.

Testing in a non-production environment

The company should test all the policies in non-production environment so as to not disrupt actual operations in case of misconfigurations. The testing should be done in an environment resembling as close as to actual production environment to ensure the policy behaviour is expected. If the company enforce the policy into the opeartional environment without any prior testing it could lead to unexpected results such as disruptions of operations, elevated access etc. in case of misconfigurations.