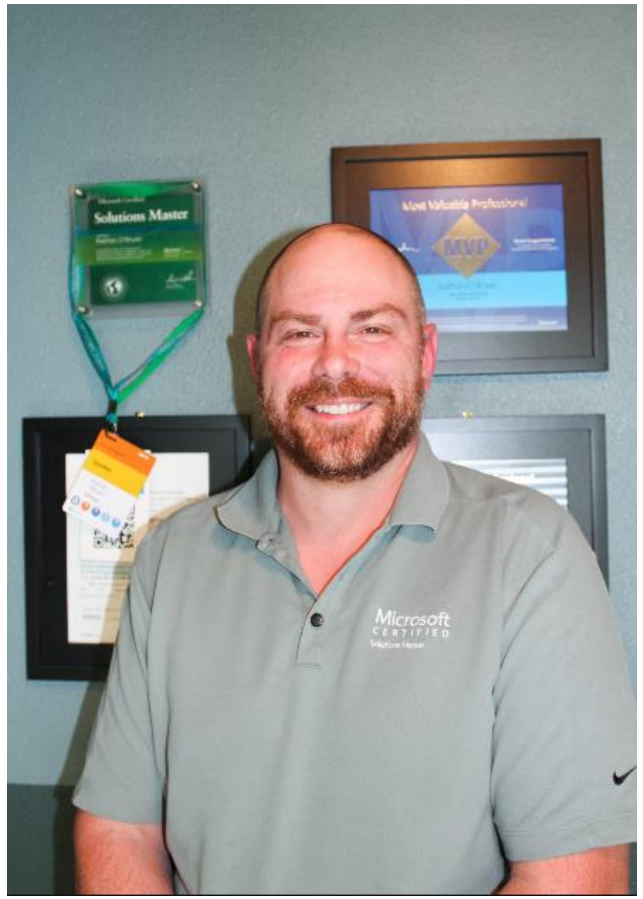
Securing Office 365 with Privileged Identity Management

Nathan O'Bryan

MVP: Office Apps and Services
MCSM: Messaging

@MCSMLab
https://www.mcsmlab.com



Security in the Cloud Era

- Shared responsibility model
- Microsoft is responsible for the infrastructure, you are responsible for your data
- Microsoft has put a lot of work into security features, we have to understand and properly implement those features
- Security is a constantly evolving requirement – we are never done!

Microsoft security

- Physical security
  - Internal datacenter networks are segregated
  - Customer data is unintelligible to those with physical access
- Logical security
  - Lockbox
  - Servers run only whitelisted code
- Data security

Microsoft security

- User controls
  - Encryption
  - Data loss prevention
  - Azure Rights Management
- Admin controls
  - MFA
  - MDM/MAM
  - Exchange Online Protection
  - Cloud App Security

Your security

- Patch!
- Understand your options
  - 1st party and 3rd party options
- Balance add-on services with cost
  - EM+S features are complex and expensive
- Auditing is your responsiblity

What is Privileged Identity Management?

- A new Azure Active Directory tool that allows you to assign “just in time” administrator rights
- Simplified auditing of changes made by administrators
- Managers don’t need to have admin privileges themselves
- Approvals can include additional documentation (reason for elevated rights, ticket information)
- 5 demos in this session

Controlling Office 365 admin rights with limited roles

- Preconfigured roles for administrators
- Limit administrators to specific job role functions
- Easy to use

Controlling Office 365 admin rights with RBAC

- Role Based Access Control
- Allows you to assign limited admin rights in Office 365 services
- Complex to customize
- Generally not used for JIT access

Azure management groups

- System for controlling multiple subscriptions within an organization
- Put subscriptions in containers and apply governance conditions to the groups

PIM PowerShell module

- Install-Module -Name Microsoft.Azure.ActiveDirectory.PIM.PSModule
- Limited cmdlets
  - Connect-PimService
  - Disable-PrivilegedRoleAssignment
  - Disconnect-PimService
  - Enable-PrivilegedRoleAssignment
  - Get-PrivilegedRoleAssignment
  - Show-PimServiceConnection

Demo 1: Start using PIM

- Configuring PIM for the first time
- License requirements
- Manage admin role assignments

Demo 2: Activate Azure AD roles in PIM

- Request activation of a role
- Activated admin rights vs normal user rights

Demo 3: PIM management with PowerShell

- Install and use PIM PowerShell module
- PowerShell cmdlets

Demo 4: PIM for Azure Resources

- Use PIM to control access to Azure resources

Demo 5: Administrators working with PIM assigned permissions

- Auditing changes
- Controlling admin rights

Thank you

- Questions?
- @MCSMLab
- https://www.mcsmlab.com