2018-12-10 azuread-govteam mtg

2018/12/10

Summary agenda:

- Updates (10m)
- Discussion topics (55m)
    - Inactive Users - final implementation review
    - Appropriate account types for AAD roles: https://wiki.cac.washington.edu/x/BJAzBQ
- Input on backlog & Future discussion topic input (5m)

-Updates on past topics & items of interest (10m)

- MS licensing project:
    - some good news on licensing we thought we were losing
    - next: stakeholder decision-making, then execution
    - **Azure AD read solution that emerged in May was deemed too impactful except for dire need**
- Dynamics 365 proof of concept by Advancement: raising tough service entanglement issues, and they will require 2FA so may be trigger
- AAD-related Incidents since 2018/10/08
    - Apps, non-impacting: 22
    - 2 Microsoft Azure MFA outages noted as not represented by INC records
- **Operational trend: 3 requests to delete guest users. Made operational decision that we won't do this–now referring callers to self-service MS doc.**
- CHG updates:
    - Complete:
        - None
    - Incomplete:
        - CHG0035494: Company administrators should enable Azure MFA for all log ins - Approved, **2 admin accounts pending** ... all other accounts 2FA enabled
        - CHG0035495: High risk AAD roles should enable Azure MFA for all log ins - Approved, no communication sent yet
        - CHG0035545: Disable inactive accounts in Microsoft infrastructure - Approved, planned start 1/9, communications start 12/10 assuming no issues identified today
    - Future?:
        - DMND0002405: UW Medicine MDM. InTune in our tenant, with shared admin of some type. Discussion with some at UW Med makes the **need for this appears less strong than previously represented** by Cris Ewell; Brad seeking clarity.
        - 'NETID DCs for hybrid cloud' analysis. **Currently exploring "bridgehead DC" option on direction of CTO**.
        - Enable Duo as custom control for demo of 2FA option
        - Enable AAD Connect * (NDA info omitted here) for demo of 2FA options
        - AAD role account type restrictions (see discussion below)
- Microsoft releases/announcements relevant to Azure AD:
    - Monthly release notes: https://docs.microsoft.com/en-us/azure/active-directory/whats-new. Note: same list is in Azure Portal "what's new" https://portal.azure.com/#@cloud.washington.edu/blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview
        - AAD logs forwardable to Azure Log Analytics (2018/10)
        - 14 new federated apps in AAD app gallery (2018/10)
        - AAD-DS email notifications released (2018/10)
        - ForceDeleteDomain API supported in Azure Portal (2018/10)
    - Not in change notes:
        - Azure AD Identity Blog: https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/bg-p/Identity
            - FIDO2 support for Microsoft accounts with Win10 1809 (2018/11)
            - Azure portal and new AAD account manager - (2018/11)
            - New AAD app registration - public preview (2018/10)
            - AAD B2C user flow improvements (2018/10)
            - Group-based licensing is GA (2018/10)
            - Hardware OATH tokens with Azure MFA - public preview (2018/10)
            - AAD sync error resolution improvements (2018/10)
        - Office 365 Blog: https://techcommunity.microsoft.com/t5/Office-365-Blog/bg-p/Office365Blog
            - None relevant
        - Microsoft 365 Blog: https://techcommunity.microsoft.com/t5/Microsoft-365-Blog/bg-p/microsoft_365blog
            - O365 earns Health Information Trust Alliance (HITRUST) CSF certification (2018/10)
        - Other
            - Customer Lockbox for Azure - public preview (2018/10)

-Discussion topics (55m)

1. Review final implementation plans for Inactive Users

Date	Action
2018/12/10	it-servicechange notification - internal to UW-IT

2018/12/12	UW-IT service center apprised
2018/12/13	compdirs, mi-announce, techsupport, MI oucontacts notification
2018/12/14	Non-person account owner/admins notification (based on analysis **now**)
Waiting period	Provides folks time to get accounts in exclusion group
2019/1/9	mi-announce, techsupport reminder notification
2019/1/9	Disable: 8 years inactivity **(Implementation starts here)**
2019/1/30	Disable: 4 years inactivity
2019/2/20	Disable: 1 year inactivity **(We're to the "new" normal operations here)**

Docs:

a. Analysis/Proposal: https://itconnect.uw.edu/wares/msinf/comm/analysis/mi-inactive-account-proposal/ (nothing new here)
b. Inactive User Design: https://itconnect.uw.edu/wares/msinf/design/users/inactive-users/ (summarizes key bits)
c. Ensure account is active: https://itconnect.uw.edu/wares/msinf/design/users/inactive-users/ensure-active/ (defines what is active, how to check, & how to get exception)
d. Re-enable my account: https://itconnect.uw.edu/wares/msinf/design/users/inactive-users/re-enable/

Draft Notification: Inactive users (Dec 2018) - Draft

2. Appropriate account types for Azure AD roles

   A strawman proposal is available at: https://wiki.cac.washington.edu/x/BJAzBQ.

   Review and discuss whether this proposal is acceptable to move forward as part of a CHG.

   Notes on where we left this:
   a. Brian introduces draft proposal for review on appropriate account types.
   b. App developer role – Lots of discussion of app developer role. Brian notes that our current configuration is in alignment with the proposed wide-open acccount type for that role.
   c. Scott raises concern about Compliance Administrator not have a more stringent recommended account type like tadm. Brian explains that Compliance Administrator has a scope limited to Office 365 apps, with something close to read permissions, so has same account type recommendation as the roles for the O365 roles.
   d. We run out of time so everyone is encouraged to review this doc, and raise questions or issues. Email the mailing list or add comments to the wiki page.
   e. Guest Inviter
      i. What's the current status of guest user access? To inform discussion, it'd help to know our current design.
      ii. What's the current authorization policy for inviting guests? e.g. only current quarter art majors (uw_major_art) are authorized to invite guests.
      iii. What accountability do we want in the guest user access process? i.e. personal vs shared accounts
      iv. Do we need to enable non-person accounts?
      v. Would use of this role ever require 2FA, either because 2FA is assigned directly to use of this role; or because 2FA is applied more widely such that use of this role requires 2FA

-Input on backlog & possible future discussion topic input (5m)

- MI activities - high level summary is high-level summary of current, planned and possible future investments, given resourcing & priority
- Possible future discussion topic list:
  - Azure AD join/hybrid join/InTune
  - Enable Password Hash Sync (for possible business continuity & to enable Microsoft signaling of known pwned accounts)
  - Azure AD Conditional Access management (this is likely to grow & there is huge potential to break things)
  - AAD token lifetime review compared to other UW tokens

Discussion Notes:

Scott asks if new operational practice on not deleting AAD guest users has customer documentation: No, not yet.

1. No feedback of significance on Inactive Users
2. Scott still feels Compliance Admin should be considered in higher protection level; Brian is happy to shift unless someone objects–no one objected.

   Minor discussion about Lockbox Admin, but decided to leave it as is.

   Scott notes that some existing accounts may need exception; notes hybrid Exchange scenario where the user is leveraging the global admin role instead of the Exchange Service Admin role.

   General satisfaction with this proposal; Brian will submit as a CHG for CAB approval.

Attending: Roland, James, Scott, Josh, Jonathan, John, Brian