2019-09-09 azuread-govteam mtg

2019/09/09

Summary agenda:

- Updates (10-15m)
- Discussion topics (50m)
    - Enable PHS sync fallback option: analysis paper (only fallback recommendation at this time)
    - AAD role approval practices and new roles: AAD role fulfillment (appropriate account types and change practices) copy--original lives in 644- MI internal docs) (please jump to "Pending" section)
    - AAD only Groups or Cloud only Exchange Distribution Lists or template for briefing
- Input on backlog & Future discussion topic input (5m)

-Updates on past topics & items of interest (10-15m)

- AAD/O365 MFA project
    - Will use Duo
    - Decisions needed: authN architecture, trigger, enablement mechanism, what Conditional Access options we'll support
    - Starting with use cases
- InTune: UWM work has stalled
- "Premium" licensing, aka A5 or other special licensing: demand stage moving to project discovery. Unclear scope or timeline.
- UW Medicine: Discussions with Slayton around AMC domain, Azure AD, and single sign on desire. May lead to significant central integration.
- 'NETID DCs for hybrid cloud' analysis. Bridgehead DC" option dead. Next steps: ExpressRoute for Microsoft Infrastructure & Azure AD Domain Services. Not yet prioritized/resourced.
- Azure AD App Proxy emerging with two apps, likely to move to production in coming months.
- CHG updates:
    - Complete:
        - CHG0035545: Inactive Users: no significant issues. Minor issues for returning staff, particularly from UWM. Minor change to allow easy re-enablement (without pwd change) was implemented.
        - CHG0035495: High risk AAD roles should enable Azure MFA for all log ins: for implementation we enable MFA by default and explore alternatives if that doesn't work.
    - Incomplete:
        - CHG0035494: Company administrators should MFA - Approved - 5 accounts MFA enabled, 2 enabled with documented exceptions, 3 accounts not MFA enabled nor exceptions recorded
    - Future:
        - CHG0037717: Azure AD Password Hash Sync Option enabled
        - CHG0037718: AAD role approval practices and new roles
- Microsoft releases/announcements relevant to Azure AD. Note: no longer exhaustive list, review the links for that; instead only highly notable items here.
    - 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
        - **8/2019: AAD custom roles for applications**
        - 8/2019: Azure Managed Identities
        - **7/2019: App-only tokens now require the client app to exist in the resource tenant**
        - 7/2019: Passwordless sign-in to Azure AD using FIDO2 security keys
        - 7/2019: Azure AD Domain Services service tag for Azure Network Security Group
        - 7/2019: B2B direct federation using SAML or WS-Fed
        - 4/2019: Access Package Workflows
        - 4/2019: Office Groups naming policy
        - 4/2019: AAD Access Reviews add features
        - 3/2019: AAD App Proxy adds support for SAML apps
    - Not in change notes:
        - Azure AD Identity Blog: https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/bg-p/Identity
            - 7/2019: Your Password doesn't matter
            - 5/2019: 16 character password limit removed
            - 5/2019: Conditional Access Authentication Session Limits
        - Office 365 Blog: https://techcommunity.microsoft.com/t5/Office-365-Blog/bg-p/Office365Blog
            - 7/2019: Activity-based expiration for Office Groups
            - 4/2019: Cloud-based OfficeProPlus policy assignment
        - Microsoft 365 Blog: https://techcommunity.microsoft.com/t5/Microsoft-365-Blog/bg-p/microsoft_365blog
            - nothing notable
        - Other
            - nothing notable

-Discussion topics (50m)

1. Enable PHS sync option - Brian
    a. Provides business continuity option
    b. Enables Microsoft signaling of known pwned accounts
    c. Required for Azure AD Domain Services
    d. May be chosen architecture via MFA project. We may be able to demo this configuration (on a per user basis) after enabling this.
2. AAD role approval practices - Brian

a. https://wiki.cac.washington.edu/x/BJAzBQ

   Notes on where we left this:
   -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 recommendation as the O365 roles. Brian extends compromise to include Compliance Administrator in higher security account grouping.

3. AAD-only groups or Cloud only Exchange Distribution Lists or template for briefing - Scott and Nathan

---

-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
  - 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
  - Hybrid Cloud update
  - Current service design
  - Vendor mgmt: what are our top 10 requests for Microsoft?
  - Azure AD service catalog entry review
  - Token revocation
  - External user - what's new & current status

Discussion Notes:

On CISO/Medicine O365 log requirements, I believe Becky et al described what meets were met through the recent meeting; and no pressing unmet needs remain?

On CHG0037717 (passwd hash sync), when we discussed which CAB mgr would approve the CHG, I recall saying "go for it" and Scott was going to approve it.

On our MI page describing high-level activities, I said I'd update the category descriptions to align with simpler current, next, future designations.

On AAD-only security groups, distribution lists, and O365 groups, Scott said he can't do business analysis, but we offered to discuss it as a topic at a future meeting.

Attending: