Active Directory Core Security Principles & Best Practices

INSIGHT SUMMIT SERIES 2018

Friedwart Kuhn & Heinrich Wiederkehr
Agenda

- Who We Are
- Intro
- Current Active Directory Threat Landscape
- Active Directory and Azure Core Security Best Practices:
  - Admin Tiering
  - Clean Source Principle
  - Hardening of Security Dependency Paths
  - Perform Security Logging and Monitoring
Who We Are

- Friedwart Kuhn
  - Head of Microsoft Security Team @ERNW
  - 15+ years experience in security assessments, administration, publications and trainings
  - IT security professional with a focus on Windows Security and Active Directory Security

- Heinrich Wiederkehr
  - Member of Microsoft Security Team @ERNW
  - 5+ years in security assessments and trainings
  - IT security professional with a focus on Windows Security and Active Directory Security
Why should you care about on-premise and cloud AD security?

- Active Directory (AD) is the main authentication backend in nearly every organization
  - Holds the keys to the crown jewels!

- AD is heavily targeted by attackers that are using powerful, publicly available tool sets

- Defence of AD environments often overlooks some typical design, implementation, configuration and operational mistakes
Why should you care about on-premise and cloud AD security?

- AD cannot be seen as a standalone entity
  - Connections to other ADs (e.g. via trust relationships) or the Cloud (e.g. via Azure AD Connect) open up new threat scenarios
  - This creates far-reaching “security dependencies”

- All security dependency paths should be in scope when securing Active Directory!
Current Active Directory Threat Landscape
Credential Theft Is Today's Crisis (James Comey)
Typical Attack Timeline & Observations

This slide is from: Mark Simos, Aaron Margosis; "Ignite 2015: Protecting against Credential Theft and Pass the Hash Today", cf. https://channel9.msdn.com/Events/Ignite/2015/BRK2334

- **First Host Compromised**
- **Domain Admin Compromised**
- **Data Exfiltration (Attacker Undetected)**
- **Attack Discovered**

**24-48 Hours**

**11-14 months**

**Attack Sophistication**
- Attack operators exploit any weakness
- Target information on any device or service

**Target AD & Identities**
- Active Directory controls access to business assets
- Attackers commonly target AD and IT Admins

**Attacks not detected**
- Current detection tools miss most attacks
- You may be under attack (or compromised)

**Response and Recovery**
- Response requires advanced expertise and tools
- Expensive and challenging to successfully recover
Paradigm Shift in Security Realities

- “Assume Breach” is the new mindset
- Identities become the new “perimeter” in the corporate network and the cloud
- The overall strategy is containment, not prevention
Relevance of Credential Theft Attacks

1. Bad guy targets workstations en masse
2. User running as local admin compromised, bad guy harvests credentials.
3. Bad guy starts “credentials crabwalk”
4. Bad guy finds host with domain privileged credentials, steals, and elevates privileges
5. Bad guy owns network, can harvest what he wants.

Example

This slide is from: Mark Simos, Nicholas DiCola; “TWC: Pass-the-Hash and Credential Theft Mitigation Architectures”
Security Dependencies May Extend Credential Theft & Reuse
Example: Pass-the-Credential via AD Trust Relationship

**Power:** Domain Controllers

**Data:** Servers and Applications

**Access:** Users and Workstations

**Trusted Domain**

**External Trust:** Unidirectional SID filtering disabled

**Trusting Domain**
Typical Reasons for Successful On-premise AD Breaches (1/2)

- Compromise via **email or browsing** almost always successful for means of an initial entry point

- From here a **Privilege Escalation** is trivial in most environments
  - Known as Credential Theft and Reuse or Pass-the-Credential

**Step 1:** Get Administrator privilege on device

**Step 2:** Read LSA secrets

**Step 3:** Use secrets to attack other devices to obtain administrator privileges
Typical Reasons for Successful On-premise AD Breaches (2/2)

- This process of Credential Theft and Credential Reuse is greatly supported by the following:
  - Lack of basic security measures
    - Insufficient patch and vulnerability management
    - User Account Control disabled
    - Local Firewalls disabled
    - Insufficient password policies
  - Legacy applications and systems which reduce overall security
    - Especially End-of-Life systems
Reasons for Azure-Relevant Breaches

- So far not so much on the Microsoft side of Azure 😊
- Bypass of MFA
  - Vulnerability: Mishandling of MFA requests.
  - Threat: If an attacker obtains a single user’s password and second factor, the attacker can use the second factor to complete the second-factor challenge for any account in the organization (CVE 2018-8340)

- More on the Azure customer admin level (see Mark Russinovich @ RSA Conference 2015 [1])
  - Internet Exposed RDP or SSH Endpoints (through weak/false Network ACL configuration)
  - Virtual Machine Missing Security Patches (through disabling of automatic updates)
  - Weak Admin/Co-Admin Credentials (through missing multifactor auth)
  - Insufficient Security Monitoring (Azure security logs & notifications not read by customer)
Positive Changes and Challenges

- Technologies exist to counter Credential Theft and Reuse
  - New features in Windows 10; e.g.:
    - Virtualization-Based Security, especially Credential Guard
    - Remote Credential Guard
    - PowerShell Logging
  - Azure security features; e.g.:
    - Azure Security Center
    - Office 365 Security & Compliance Center

- Microsoft expands Azure security services aimed at improving customer security in Azure (Password Protection, Attack Simulator, etc.)

- Security awareness regarding AD and Azure seems to increase
  - There is a reason why you are here ;)

Active Directory and Azure Core Security Best Practices
Active Directory and Azure Core Security Best Practices

- Admin Tiering
- Clean Source Principle
- Hardening of Security Dependency Paths
- Security Logging and Monitoring
Administrative Tier Model

Admin Tiering in a Nut Shell
The Problem: Admins Logging on Everywhere...
The Solution: Implement Administrative Tiers

Tier 0
- Domain Controllers, Domain Admin
- Workstations, Special Tier 0 Systems (Patch, AV, Mgmt)
- BUILTIN\Administrators
- General: Tier 0 Admins

Tier 1
- Application Servers
- Server/App Admin
- Workstations, Tier 1 Mgmt Systems
- Server Admins, Server Services
- Application Admins
- General: Tier 1 Admins

Tier 2
- Internet Connected
- Workstations of Standard Users
- Workstation Admins (Tier 2 Admins)

Tier 3
- Standard Users
**Tier Model Principles**

**Classify:** Every single security principal, system, or application has to be classified as belonging only to one tier

**Restrict Logons:** Security principals of a higher tier must never log on to a resource on a lower tier (→ Implement logon restrictions)

**Restrict Control:** Security principals of a lower tier must never control resources of a higher tier (→ Implement control restrictions)
Implementation of Tier Model Principles

1. Classify/reorganize the content of each tier (accounts, systems/applications)

2. Implement two kinds of restrictions
   - **Control restrictions**
     - define, which identities control assets on which tiers (via System Privileges and NTFS Rights)
     - and thereby **mitigate privilege escalation**
   - **Logon restrictions**
     - define, which identity is allowed to logon to which tier
     - and thereby **mitigate credential exposure**
The objective of control restrictions is to **prevent privilege escalation** in Active Directory:
- Administrators (and other accounts) of a lower tier should not be able to control systems, applications and accounts of a higher tier.
  - Sample: If a server operator on a member server is member of the Enterprise Administrators group, he controls DCs. (This should not be the case.)

Control restrictions of an account (administrative account, service account) refer to:
- Group membership in Active Directory
- Rights on Active Directory objects
- SID-History attribute
- Local group membership
- System privileges
- NTFS rights
- Registry rights
Control Restrictions vs. Logon Restrictions

- Same Tier Control
- Lower Tier Control Only as Required by Role
- Higher Tier Control Blocked

Same Tier Logon
Higher Tier Logon
Lower Tier Logon
Blocked
Only as Required by Role
Tier 0 administrators manage tier 0 assets like...

- Domain Controllers
- Identity stores (Active Directory database)
- A small number of systems and identities in Tier 0, such as: PKI, patch management, AV, backup, virtualization (all of them exclusively for Tier 0)

...and:

- Can manage and control assets at any level as required by the role (e.g. management of group membership in Active Directory in all tiers, management of GPOs that affect all tiers)
- Tier 0 administrators only log on interactively or access assets trusted at the Tier 0 level
Tier 1 administrators manage assets of Tier 1 like...
- enterprise servers (file servers, database servers, virtualization components etc.)
- services (patch management, AV, backups etc.)
- applications (SAP etc.)
- Tier 1 accounts

...and:
- Can only manage and control assets at the Tier 1 or Tier 2 level in the compartment, where the admin is allowed to administer
- Can only access assets (via network logon type) that are trusted at the Tier 1 or Tier 0 levels
- Should only interactively log on to assets trusted at the Tier 1 level (within their compartment – if compartments are defined)
Tier 2 administrators manage assets of Tier 2 like...
- enterprise desktops, laptops and printers
- other user devices like scanners, removable media etc.

...and:
- Can only manage and control assets at the Tier 2 level in the compartment, where the admin is allowed to administer
- Can access assets (via network logon type) at any level as required
- Can only interactively log on to assets trusted at the Tier 2 level
Tier 3 contains:

- standard users without administrative privileges
- users which need local administrative privileges over a single computer (or a very small number of computers) of Tier 2
  - typical (local admin) users are: developers, sometimes VIPs
Administrative Tier Model in Azure (?)!

- Credential theft and privilege escalation are relevant for Azure too... So are Administrative Tiers ;-)

- Administrative Tiers in Azure are in *any case* relevant security controls
  - In case of an extension of your on-prem AD to Azure
  - In case of a potential future connection between your on-prem AD and Azure
  - Even in case of a complete separation of your on-prem AD and Azure
Administrative Role Types in Azure You Have to Keep in Mind...

- Azure AD roles (tenant-wide)
  - Over 30 roles for administration of Identities, Applications, Devices and SaaS (such as Office 365)

- Azure “classic” administration model
  - Account Administrator (tenant-wide), Service Administrators and Co-Administrators (subscription-wide)

- Azure Resource Manager model (Azure RBAC) roles
  - Over 70 fine-grained administrative roles for administration of Azure resources
Tier 0 Equivalency in Azure

- Identities that grant the possibility to take control over an Azure tenant, have to be considered Tier 0.

- Tier 0 equivalency in Azure corresponds to the following accounts:
  - Account Administrator
  - Global Administrator (AAD role)
  - Privileged Role Administrator (AAD role)
  - Billing Administrator (Update organization.trustedCAsForPasswordlessAuth property in Azure Active Directory) (AAD role)
  - Application Administrator (AAD role)
Tier 1 Equivalency in Azure

- Most Azure and Office 365 resources can be seen as equivalent to on-premise assets like:
  - Enterprise servers (file servers, database servers, virtualization components etc.)
  - Services (patch management, AV, backups etc.)
  - Applications (SAP etc.)
- ... and therefore as Tier 1
  - The administrators controlling the subscriptions and resources as well as most administrative roles in Azure AD that are not considered Tier 0 also have to be placed in Tier 1
Tier 2 Equivalency in Azure

- The management of standard users is handled in Azure AD by
  - User Account Administrator
  - Password Administrator
  - Licence Administrator

- Windows 10 machines joined to Azure AD are controlled in Azure AD by
  - Cloud Device Administrator
    - Enable, disable and delete in Azure AD
    - Read Bitlocker Encryption keys
  - Device Administrators
    - Additional local administrator of the devices

- But be careful as standard users in Azure AD can be authorized to have administrative privileges in Azure or Office 365 subscriptions
Implementation Steps of Admin Tiers in Azure

- Same as in on-prem Active Directory
- Every single security principal, system, or application has to be **classified** as belonging only to one tier
- Implement **control restrictions**
  - Via AAD administrative roles and RBAC model roles
- Implement **logon restrictions** to prevent
  - Tier 0 Azure accounts from logging on to non-Tier 0 VMs such as
    - AAD-joined (physical) Win10 devices
    - VMs and (customer applications) in Azure
    - Azure AD DS-joined VMs
Example: Admin Tiering for Tier 0 Asset Extended to Azure

Tier 0 subscription administrators should be sourced from members of the Active Directory Domain Administrators. Access to VHD storage, ability to provision virtual machine agents, ability to modify Security Group rules, all contribute to making subscription admins De-Facto domain administrators.

Workload subscriptions' administrators should not be subscription administrators in the Tier 0, active directory, subscription.

An on-premises resource forest/domain extended to Azure. Alternatively, a dedicated Azure resource forest could be created. Necessary network connectivity required.

Admin Tiering in Hybrid ADs – Recommendations

- Don’t mix on-prem AD-Administration with Azure Administration
  - Use on-prem AD identities for on-prem AD administration
  - Use Azure identities for Azure Administration
  - Don’t mix on-prem Admin Tiers with Azure Admin Tiers

  ⇒ Consider *not syncing* on-prem admins of T0, T1, T2 to Azure
  ⇒ Consider *not extending* T0 into Azure (use instead Azure AD Domain Services)
  ⇒ Consider *separate T1 admins* for on-prem domain-joined servers in Azure
Summary Admin Tiering

- The most important and comprehensive security control for Active Directory and hybrid ADs with respect to credential theft, credential reuse and privilege escalation
- Basis for many other technical controls
- Industry standard (Windows) administration model
- Requires modification in admin mindset
- Admins will have more accounts and hence higher operational effort
- Applies to Azure too!
- But on-prem vs. Azure Admin Tiers need to be well understood and separated
- Alternatives
  - None
Clean Source Principle
The Problem: Security Dependencies

- In a security dependency the subject might not be as trustworthy as the object being secured. For example:

  - **OS or Application Install**: Compromise Vector
  - **Installation Media**: Administration Task
  - **User Workstation**: Compromise Vector
  - **Infect Media**: OS or Application Install
  - **Infect Workstation**: Installation Media
The Solution: Clean Source Principle

- Any subject in control of an object is a security dependency of that object
  - The assurances for all security dependencies must be at or above the desired security level of the object itself
  - **Control is transitive!** (For example if A controls B and B controls C, then A also indirectly controls C.)

- Most common areas of control are:
  - the hardware where systems are installed,
  - the installation media for the systems,
  - the architecture and configuration of the system,
  - and daily operations.
Clean Source Principle: Installation

- Ensure that the installation media has not been tampered with
  - Requires validating the software integrity throughout the lifecycle including during acquisition, storage, and transfer until usage

- The source of the software must be validated
  - Physical media directly from the vendor
  - File hash validation
  - Revocation checks for digital signatures

- The software must be stored in a location that is protected from modification
  - especially by internet-connected hosts
  - or personnel trusted at a lower level than the systems where the software system will be installed
Clean Source Principle: Administration

- Provide a dedicated secure administration environment for sensitive tasks that is protected from Internet attacks and sophisticated threat vectors
  - On an operating system level: Implement Privileged Access Workstations (PAW)
  - On an Active Directory level: Implement Enhanced Security Administration Environment (ESAE) and/or PRIV Forest(s)

- Extension of the recommended practice to use separate admin and user accounts for administrative personnel
  - Separates sensitive tasks and accounts from the daily use workstations and devices
  - Strong protection from phishing attacks, application and OS vulnerabilities, and various impersonation attacks (e.g. Pass-the-Hash or Pass-the-Ticket)
Clean Source Principle: PAWs

- PAW hardware profiles can be:
  - Dedicated hardware
    - Separate dedicated devices for user tasks vs. administrative tasks
  - Simultaneous use
    - Single device that can run user tasks and administrative tasks concurrently by taking advantage of OS or presentation virtualization. For example:
      - Adding a local user VM
      - Adding RemoteApp, RDP, or a VDI
Clean Source Principle: ESAE/PRIV Forest

- Dedicated administrative forest
  - Hosts administrative accounts, workstations, and groups
  - Environment has stronger security controls than the production environment

- **ESAE forest** moves all sensitive objects for Tier 0 administration to a separate forest (except the krbtgt account)

- **PRIV forest** moves administrative identities for Tier 1 & 2 administration to a separate forest and combines this with a PAM solution (e.g. MIM 2016)
Exemplary Secure Administration Environment Models

- Option 1:
  - Tier 0 managed exclusively via PAWs

- Option 2:
  - Tier 0 managed by a Local ESAE Forest

- Option 3:
  - Tier 0 managed by a Global ESAE Forest

- All options can be combined with a PRIV Forest
Clean Source Principle in Azure (Administration)

- Administration of high-value Azure assets also requires the use of PAWs
  - Alternatives do not exist
  - Microsoft also does this for all on-premise and Azure resources!

- Hardening the access path becomes more important
  - Management of resources does not only take place inside your own network, but also over the Internet
  - Securing the “edge” becomes a priority
**Secure Admin Workstation: Enforcements**

Comprehensive layers of enforcement controls, enabling authorized access for only healthy and secure admin workstation devices to on-premises resources and through-out the cloud.

**What is enforcement?**

- **IP Based Isolation**
  - Traditional network-based isolation using IP range, firewall and route ACL’s to ensure access from only trusted subnets and IP addresses.

- **Machine Identity**
  - Machine based identity perimeter(s) enabling access based on client computer account, group membership or domain membership.

- **User Identity**
  - User based identity perimeter(s) enabling access based on user account or (active) group membership.

- **Health and Compliance State**
  - Identity based perimeters layered with device health attestation, ensuring...

**HRE EDGE**

- High Risk Environment hosting
  - Additional security controls above and beyond industry standards:
    - FTE only access, ICS 705,
    - Physical Admin Access only

**AAD Conditional Access**

- Identity Access allowed based on Source IP

**AD User/Group**

- Identity / Role based access on resource

**Network ACL**

- IP based access based on route/firewall ACLs

**IPSEC: User & Machine based access**

- User & Machine based access

**Proxy / Web service**

- User/Role based explicit URL/website access

**Proxy / Web service**

- User/Role based explicit URL/website access

**IP Based ACLs**

- Resources are ACL’s based on SAW Source IPs

**Hardware based Health and Compliance Assurance**

- TPM 2.0
- Secure Boot
- Windows 10 Device Guard
- Windows 10 Credential Guard
- Host Guardian Service (HGS)
- SmartCard Credential
- TPM based VPN Connectivity
- BIOS locked configuration
- OS Update Compliance

See: [2]
Special Clean Source Principle Measures for Azure Administrators

- Use Azure Multi-Factor Authentication (MFA)
  - "Only 0.73% of tenant admins have Multi-factor Authentication enabled" (Microsoft Ignite 2017 BRK3016)
  - Should be required at least for all individual users who are permanently assigned to one or more of the Azure AD admin roles: Global administrator, Privileged Role administrator, Exchange Online administrator, and SharePoint Online administrator
  - Ideally, enabled for all Azure AD admin roles

- Use work accounts instead of Microsoft accounts
  - Microsoft accounts should be replaced by individual cloud-based or synchronized accounts

- Global administrator accounts should not have personal email addresses
Clean Source Principle in Azure (Software Installation)

- Installation of software or usage of downloaded data should follow the same principles as in the on-premise AD
  - New sources of software are available in the form of the Azure Marketplace
  - The marketplace provides various forms of “product types”:
    - SaaS
    - Solution Templates
    - VM Images

- Pay special attention to VM images for IaaS from the Azure Marketplace as they are often outdated!
Cloud marketplaces are supply chains

- Supply chain attacks are increasingly common
- Cloud marketplaces could be next
- Lots of resources; high value targets
- Minimal validation of 3rd party IaaS VM images
- 3rd party IaaS images are OLD
  - Average Azure Age: 123 days
  - Average AWS Age: 717 days
- Updating IaaS VM images is not retroactive

Make The World A Safer Place - #TR18
Hardening of Security Dependency Paths
Hardening Security Dependency Paths?

- Clean Source Principle covers hardening of security dependencies
  - The source must be “clean”

- But what about the actual control relationship?
  - In many cases the “connection” between a subject and an object can also be hardened
Active Directories typically consist of more than one interconnected domain/forest.
Security of AD Trust Relationships

- Every trust relationship to foreign ADs will impact the security of the own AD
  - Regardless of the trust direction!

- The trust direction influences whether identities or resources are exposed to the trusted/trusting AD
Hardening of AD Trust Relationships

- **Prerequisite:** All ADs that have connections via trusts should ideally also implement administrative tiers
  - If necessary, the tiers of the source AD can be extended into the connected AD and
  - Guarantees an comparable level of security
Hardening of AD Trust Relationships

- When the need for a trust has been established, the following questions should be asked:
  - Which direction of the trust is technically required?
    - Unidirectional trusts should always be preferred
  - Is the trust required for a migration project? Must SID filtering be disabled?
    - SID filtering on external trusts should always be enabled
    - Forest trusts should not be treated as external trusts with regards to SID history and SID filtering
  - Should all users of the trusted domain/forest be able to access all resources of the trusting domain forest?
    - Selective Authentication should be enabled if technically and operationally feasible
Hardening of AD Trust Relationships

- After the aforementioned questions have been clarified:
  - Results should be documented
  - Trust should be configured accordingly
  - Trust configuration should be regularly reviewed based on the documentation to catch drift
Means of Control in Azure

**Important:** upstream control also includes hosts where upstream administrator credentials are used/exposed.

Hardening of Azure Connections

- Hardening Azure AD Connect accounts and systems
- Hardening of AD FS
- Hardening of Pass-through Authentication
Hardening Azure AD Connect Accounts and Systems

- System(s) running Azure AD Connect sync engine and corresponding SQL database should be treated and hardened as Tier 0 system(s)
  - Don’t forget the basics, e.g. patching of Azure AD Connect

- The ADSync service account should run as a Virtual Service Account or at least a Group Managed Service Account, but not a normal user account

- The AD DS Connector Account should be hardened in accordance with Microsoft Security Advisory 4056318
AD DS Connector Account

- With express settings created with prefix MSOL_
- Has a long complex password that does not expire
- Used to read/write information to Windows Server Active Directory
- Not protected through the AdminSDHolder object
- Created directly under the on-premises AD User container
  - Therefore a member of the Account Operators group can escalate his privileges

<table>
<thead>
<tr>
<th>Permission through Express Installation</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replicate Directory Changes</td>
<td>Password hash sync</td>
</tr>
<tr>
<td>Replicate Directory Changes All</td>
<td></td>
</tr>
<tr>
<td>Read/Write all properties User</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties iNetOrgPerson</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Group</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Contact</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Reset password</td>
<td>Preparation for enabling password writeback</td>
</tr>
</tbody>
</table>
AD DS Connector Account

- Microsoft addressed this in Microsoft Security Advisory 4056318. The recommendations are as follows:
  - Use of Account Operators group should be avoided
  - Move the AD DS account used by Azure AD Connect into an OU that is only accessible by trusted or highly-privileged administrators
  - When delegating Reset-Password permission to specific users, scope their access to only user objects for which they are supposed to manage
  - Lock down of access to the AD DS account by implementing permission changes in the on-premises AD (see next slide)
    - Azure AD Connect version 1.1.654.0 (and after) implements these changes but a upgrade will not retroactively apply these changes
AD DS Connector Account

- Lock down of access to the AD DS account by implementing permission changes in the on-premises AD
  - Disable Access Control List inheritance on the object
  - Remove all default permissions on object except for SELF
  - Implement the permissions on the right

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Access</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>SYSTEM</td>
<td>Full Control</td>
<td>This object</td>
</tr>
<tr>
<td>Allow</td>
<td>Enterprise Admins</td>
<td>Full Control</td>
<td>This object</td>
</tr>
<tr>
<td>Allow</td>
<td>Domain Admins</td>
<td>Full Control</td>
<td>This object</td>
</tr>
<tr>
<td>Allow</td>
<td>Administrators</td>
<td>Full Control</td>
<td>This object</td>
</tr>
<tr>
<td>Allow</td>
<td>Enterprise Domain Controllers</td>
<td>List Contents</td>
<td>This object</td>
</tr>
<tr>
<td>Allow</td>
<td>Enterprise Domain Controllers</td>
<td>Read All Properties</td>
<td>This object</td>
</tr>
<tr>
<td>Allow</td>
<td>Enterprise Domain Controllers</td>
<td>Read Permissions</td>
<td>This object</td>
</tr>
<tr>
<td>Allow</td>
<td>Authenticated Users</td>
<td>List Contents</td>
<td>This object</td>
</tr>
<tr>
<td>Allow</td>
<td>Authenticated Users</td>
<td>Read All Properties</td>
<td>This object</td>
</tr>
<tr>
<td>Allow</td>
<td>Authenticated Users</td>
<td>Read Permissions</td>
<td>This object</td>
</tr>
</tbody>
</table>
Hardening of AD FS

- OS Hardening as a basis
- Treat the AD FS server as a Tier 0 system
- Use of Web Application Proxy (WAP)
  - Only open necessary ports on the firewall
  - Limit number of endpoints enabled on the proxy
- Use the “Extended Protection for Authentication” feature
- Use Extranet lockout protection
- Require MFA (at least for admins)
- The keys used to sign the tokens can be protected in a HSM
Hardening of Pass-through Authentication

- A compromise of the servers running authentication agents would expose the Azure resources
  - Should be treated as Tier 0 systems
- No need to open ports on the firewall for inbound communication
  - So only open the necessary ports for outbound communication
- Patching and certificate renewal is handled by Microsoft
Security Logging and Monitoring
Design & Implement Active Directory- and Azure AD-specific Logging & Monitoring

- Vast topic that will not be covered in this talk but needs to be designed and implemented
- In on-prem AD this means:
  - Definition of (at least) two (advanced) audit policies (baseline & high security audit policy)
  - Definition of event IDs to be gathered and transferred to the SIEM **and** evaluated by dedicated personnel
  - A focus should be laid on logon and control restriction violations attempts
Enhanced Visibility with Azure

- Azure provides basic capabilities to monitor identity activity out of the box.

- Microsoft offers a wide array of services to improve the visibility of security-relevant activity in Azure. These are mainly:
  - Azure Active Directory Identity Protection
  - Azure Monitor
  - Azure Security Center

- In addition, Microsoft informs you in severe cases if your Azure tenant is under attack or an attack is originating from your tenant.
  - Keep your contact information up-to-date!
Azure Monitoring Basics

- Monitor Changes in your Tenant
  - Monitor changes to roles and group memberships
  - Monitor changes to authentication methods for privileged accounts
  - Regularly review the Risky Sign Ins report
  - Use Access Reviews for applications
Thank you for your time!

fkuhn@ernw.de
hwiederkehr@ernw.de

www.ernw.de

www.insinuator.net
Sources


- [2]: https://myignite.techcommunity.microsoft.com/sessions/65954?source=sessions

- Icons
  - https://icons8.com/
Additional Material & Information
Example: User Account Administrators and Enterprise Application Owners (Issue)
Example: User Account Administrators and Enterprise Application Owners (Possible Solution)
Implementation Guidelines

- Begin with Tier 0
  - Followed by Tier 1 and then Tier 2
- Use compartments in Tier 1
- Do not let service accounts undermine the Administrative Tier model
- Provide admins with detailed technical guidelines (about the consequences of logon & control restrictions)
- Build equivalent Tiers in Azure
  - Begin with Tier 0, followed by Tier 1 (as well with compartments) and Tier 2
  - Don’t mix on-prem Admin Tiers with Azure Admin Tiers
- Assume a long-term project