AYI NEDJIMI Consultants

Sécuriser Microsoft Entra ID : Conditional Access, MFA

Catégorie : Microsoft 365 Lecture : 12 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide complet de sécurisation Microsoft Entra ID : Conditional Access policies, MFA avancé, protection des identités, détection des compromissions et.

Face à cette réalité, la sécurisation d'Entra ID ne relève plus d'un simple paramétrage technique : elle constitue un **programme stratégique** qui engage l'architecture Zero Trust, la gouvernance des accès et la capacité de détection de l'organisation. Ce guide explore en profondeur les mécanismes de protection disponibles -- Conditional Access, MFA avancé, Identity Protection, Privileged Identity Management -- et propose une méthodologie de durcissement applicable immédiatement. Guide complet de sécurisation Microsoft Entra ID : Conditional Access policies, MFA avancé, protection des identités, détection des compromissions et. Microsoft 365 est omniprésent en entreprise et sa surface d'attaque ne cesse de s'étendre. La sécurisation de securiser entra id conditional access nécessite une approche structurée et des outils adaptés. Nous abordons notamment : 8. checklist de durcissement : 20 points essentiels, gestion des identités entra id et questions frequentes. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

L'objectif est double : d'une part, fournir aux architectes sécurité et administrateurs M365 un référentiel technique complet ; d'autre part, proposer aux RSSI et décideurs une vision structurée des contrôles à prioriser. Chaque section intègre des recommandations concrètes, des exemples de configuration et des liens vers les articles connexes de notre base de connaissances. Nous abordons également les erreurs fréquentes observées lors de nos audits -- des configurations qui semblent sécurisées mais qui laissent des failles exploitables par un attaquant déterminé.

Point clé : La sécurisation d'Entra ID est un processus continu. Microsoft déploie en moyenne 15 à 20 nouvelles fonctionnalités de sécurité par trimestre. Rester à jour n'est pas optionnel -- c'est une obligation pour maintenir une posture défensive efficace.

Prérequis de cet article

Cet article suppose une connaissance de base d'Entra ID et de l'écosystème Microsoft 365. Pour une introduction aux applications enregistrées dans Azure AD et aux mécanismes d'authentification OAuth, consultez nos articles dédiés.

Avez-vous vérifié les permissions effectives de vos comptes de service Azure AD ?

Entra ID utilise un modèle RBAC (Role-Based Access Control) avec plus de **90 rôles intégrés**. Les plus critiques du point de vue sécurité sont :

- **Global Administrator** : accès total au tenant. Ce rôle doit être limité à 2-4 comptes maximum, protégés par MFA résistant au phishing et PIM.

- **Privileged Role Administrator** : peut gérer les attributions de rôles dans Entra ID. Aussi sensible que le Global Admin dans la pratique.
- **Security Administrator** : gère les politiques de sécurité, Identity Protection, Conditional Access. Rôle critique mais souvent surattribué.
- **Application Administrator** : gère toutes les inscriptions d'applications et les service principals. Peut créer des credentials pour n'importe quelle application, un vecteur d'attaque majeur.
- **Exchange Administrator / SharePoint Administrator** : accès aux données métier. La compromission de ces rôles donne accès à l'ensemble des communications et documents de l'organisation.

L'erreur la plus fréquente que nous observons en audit : l'**attribution permanente de rôles Global Administrator** à 10, 15, voire 20 comptes. Chaque compte GA permanent est une cible de choix pour un attaquant. La solution : **Privileged Identity Management (PIM)**, que nous détaillerons en section 6.

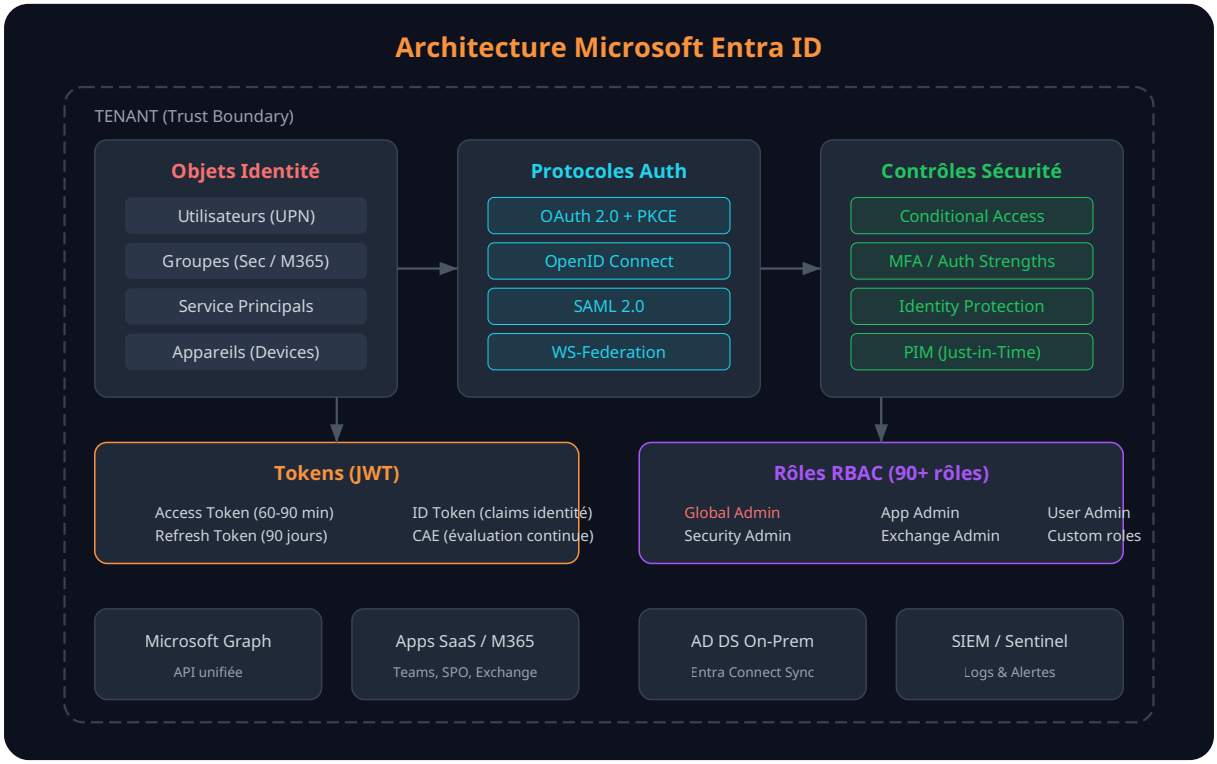

Figure 1 -- Architecture Microsoft Entra ID : objets, protocoles, contrôles de sécurité et intégrations

Les protocoles legacy (IMAP, POP3, SMTP Auth, Exchange ActiveSync legacy) ne supportent pas le MFA et constituent un vecteur d'attaque privilégié pour le password spraying et le credential stuffing. Une politique de blocage strict est indispensable :

```
// Pseudo-configuration CA Policy - Block Legacy Auth
Assignments:
  Users: All users (aucune exclusion)
  Cloud apps: All cloud apps
  Conditions:
    Client apps: Exchange ActiveSync, Other clients

Grant:
  Block access
```

Piège fréquent : les exclusions legacy
Lors de nos audits, nous trouvons régulièrement des exclusions "temporaires" pour des imprimantes multifonctions, des applications métier legacy ou des boîtes partagées qui utilisent encore SMTP Auth. Ces exclusions sont des **portes ouvertes pour le password spraying**. La solution : migrer vers OAuth 2.0 (SMTP AUTH OAuth pour les imprimantes modernes) ou isoler ces comptes avec des mots de passe longs et aléatoires, sans aucun rôle ni accès aux données sensibles.

Politique 3 : Exiger des terminaux conformes pour les applications sensibles
Pour les applications contenant des données sensibles (Exchange Online, SharePoint, Teams), l'accès devrait être limité aux terminaux gérés par Intune et conformes aux politiques de sécurité (chiffrement disque, antivirus à jour, OS patché). Cette politique combine les contrôles **"Require device to be marked as compliant"** et **"Require Hybrid Azure AD joined device"** en mode OR (l'un ou l'autre suffit) pour couvrir à la fois les terminaux cloud-only et les postes joints au domaine.

Politique 4 : Renforcement basé sur la localisation
Les **Named Locations** permettent de définir des réseaux de confiance (IP ranges du siège, VPN, datacenters) et des pays autorisés. Une politique efficace combine :

- **Blocage des pays non autorisés** : bloquer tout accès depuis les pays où l'organisation n'a aucune activité. Cela stoppe une grande partie des attaques par password spraying originaires de certaines régions.
- **MFA renforcé hors réseau de confiance** : exiger un MFA phishing-resistant pour tout accès ne provenant pas d'une named location de confiance.
- **Attention au GPS spoofing** : les locations basées sur l'IP sont plus fiables que la géolocalisation GPS. Combiner avec la conformité du terminal pour une protection plus robuste.

Entra ID supporte trois types de passkeys :

- **Clés de sécurité matérielles** (YubiKey, Feitian, etc.) : recommandées pour les administrateurs et comptes à haut privilège. Résistantes à la compromission du terminal.
- **Passkeys liées à la plateforme** (platform authenticators) : Windows Hello, Touch ID/Face ID, Android biometrics. Idéales pour le déploiement à grande échelle sur les terminaux gérés.
- **Passkeys synchronisées** (synced passkeys) : synchronisées via iCloud Keychain, Google Password Manager, ou Microsoft Authenticator. Plus pratiques mais avec un modèle de confiance élargi (la sécurité dépend du compte Apple/Google).

4.4 Temporary Access Pass (TAP) et scénarios d'onboarding

Le **Temporary Access Pass** résout un dilemme classique : comment enregistrer une méthode MFA phishing-resistant quand l'utilisateur ne peut pas encore s'authentifier avec MFA ? Le TAP est un code temporaire (durée configurable, de 10 minutes à 30 jours) avec un nombre d'utilisations limité (par défaut une seule utilisation).

Les cas d'usage principaux :

- **Onboarding d'un nouvel employé** : le service IT génère un TAP qui permet au nouvel utilisateur de s'authentifier une première fois et d'enregistrer sa passkey FIDO2 ou son Windows Hello.
- **Récupération après perte de device** : lorsque l'utilisateur a perdu toutes ses méthodes MFA (téléphone et clé de sécurité), un TAP permet la réinitialisation sans compromettre la sécurité.
- **Migration vers le passwordless** : TAP comme pont temporaire pendant la transition des comptes vers l'authentification sans mot de passe.

Configuration TAP recommandée
Limitez la durée du TAP à **1 heure maximum**, avec une seule utilisation autorisée. Exigez que les TAP ne puissent être créés que par des rôles Authentication Administrator ou supérieur, avec une journalisation complète. Vérifiez que le TAP est bien configuré en tant que méthode **one-time use** pour éviter qu'un TAP intercepté puisse être réutilisé.

4.5 Authentication Strengths : piloter la granularité du MFA

Les **Authentication Strengths** (forces d'authentification) permettent de définir précisément quelles combinaisons de méthodes MFA sont acceptables pour chaque politique Conditional Access. Trois niveaux prédéfinis existent :

- **MFA strength** : accepte toute combinaison de deux facteurs (Authenticator push, TOTP, SMS, etc.).
- **Passwordless MFA strength** : requiert des méthodes sans mot de passe (Windows Hello, Authenticator passwordless, passkeys FIDO2).
- **Phishing-resistant MFA strength** : le niveau le plus élevé, restreint aux méthodes résistantes au phishing (FIDO2, Windows Hello for Business, Certificate-based authentication).

Il est possible de créer des **Authentication Strengths personnalisées** pour des scénarios spécifiques. Par exemple, pour les administrateurs Global Admin, vous pouvez créer une force qui n'accepte que les clés FIDO2 matérielles d'un fabricant spécifique (en filtrant par AAGUID), excluant ainsi les passkeys synchronisées ou les platform authenticators potentiellement moins sécurisés dans votre contexte.

```
// Exemple de requête Graph pour créer une Authentication Strength personnalisée
POST /beta/policies/authenticationStrengthPolicies
{
  "displayName": "Admin FIDO2 Hardware Only",
  "description": "Clés FIDO2 matérielles uniquement pour les admins",
  "allowedCombinations": [
    "fido2"
  ],
  "combinationConfigurations": [{
    "@odata.type": "#microsoft.graph.fido2CombinationConfiguration",
    "allowedAAGUIDs": [
      "cb69481e-8ff7-4039-93ec-0a2729a154a8",  // YubiKey 5
      "ee882879-721c-4913-9775-3dfcce97072a"   // YubiKey 5 NFC
    ]
  }]
}
```

La puissance d'Identity Protection réside dans sa capacité d'**auto-remédiation**. En couplant les détections de risque aux politiques Conditional Access, l'organisation peut automatiser la réponse aux compromissions sans intervention humaine :

Scénario de risque	Action automatique	Impact utilisateur
Sign-in risk = Medium	Exiger MFA	L'utilisateur complète son MFA et continue. Si c'est un attaquant sans le second facteur, il est bloqué.
Sign-in risk = High	Exiger MFA phishing-resistant	Seules les clés FIDO2 / WHfB sont acceptées. Bloque les attaques AitM.
User risk = Medium	Exiger MFA + changement de mot de passe	L'utilisateur doit prouver son identité via MFA puis changer son mot de passe.
User risk = High	Bloquer l'accès	Le compte est bloqué jusqu'à intervention d'un administrateur qui enquête et remédie manuellement.

5.3 Investigation et tuning des détections

Identity Protection nécessite un **tuning continu** pour réduire les faux positifs sans affaiblir la détection. Les actions clés :

- **Déclarer les Named Locations** : les IP de VPN, les plages des bureaux et des datacenters doivent être déclarées comme trusted locations pour éviter les alertes "Unfamiliar sign-in properties" et "Impossible travel" sur les accès légitimes via VPN.
- **Exclure les service accounts** : les comptes de service utilisés pour l'automatisation (Graph API, PowerShell) peuvent générer des alertes "Anomalous token" ou "Suspicious API traffic". Utilisez des **managed identities** quand c'est possible, ou excluez ces comptes des politiques de risque utilisateur (tout en les surveillant par d'autres moyens).
- **Revue régulière des utilisateurs à risque** : planifiez une revue hebdomadaire du rapport "Risky users" pour investiguer les comptes en état "At risk" et confirmer ou dismiss les détections.

- **Corrélation avec le SIEM** : exportez les détections Identity Protection vers votre SIEM (Sentinel, Splunk, etc.) pour corréler avec d'autres sources de données (logs réseau, EDR, proxy).

Attention aux faux positifs d'Impossible Travel
L'impossible travel est la détection qui génère le plus de faux positifs. Un utilisateur qui se connecte via le WiFi du bureau (IP française) puis via le VPN corporate (IP sortie aux Pays-Bas) peut déclencher une alerte. De même, l'utilisation d'un proxy CASB peut modifier l'IP de sortie. Ajustez les named locations en conséquence et n'utilisez pas "Impossible travel" comme seul critère pour bloquer un accès.

L'export des logs Entra ID vers un SIEM est indispensable pour une détection efficace. **Microsoft Sentinel** offre l'intégration la plus native via le connecteur Entra ID (anciennement Azure AD), mais des connecteurs existent pour Splunk, QRadar, Elastic, et tout SIEM compatible CEF/Syslog.

Les **règles de détection critiques** à implémenter en priorité :

- **Connexion réussie d'un compte break-glass** : alerte CRITIQUE immédiate. Toute utilisation d'un break-glass en dehors d'un test planifié doit déclencher une investigation.
- **Attribution de rôle Global Administrator** (permanent) : alerte HAUTE. Doit passer par PIM -- une attribution permanente directe est suspecte.
- **Ajout de credentials à un service principal** : alerte HAUTE. Un attaquant ajoute souvent un secret ou un certificat à une application existante pour maintenir son accès.
- **Modification d'une politique Conditional Access** : alerte MOYENNE. Vérifier que le changement est autorisé et documenté.
- **Consentement admin-wide à une application** : alerte HAUTE. Le consent phishing est un vecteur d'attaque majeur documenté dans notre article sur les applications enregistrées Azure AD.
- **Volume anormal d'échecs de connexion** depuis une même IP : alerte MOYENNE. Indicateur de password spraying.
- **Désactivation du MFA** pour un utilisateur à privilèges : alerte HAUTE. Peut indiquer une tentative de préparation d'attaque.
- **Création d'une règle de transfert Exchange** ou d'une règle inbox : alerte MOYENNE. Technique classique de BEC (Business Email Compromise).

```
// Exemple de requête KQL pour Sentinel - Détection d'attribution Global Admin
AuditLogs
| where TimeGenerated > ago(1h)
| where OperationName == "Add member to role"
| where TargetResources[0].modifiedProperties[0].newValue
    contains "Global Administrator"
| where Result == "success"
| project TimeGenerated, InitiatedBy.user.userPrincipalName,
    TargetResources[0].userPrincipalName, OperationName
| sort by TimeGenerated desc
```

7.3 Workbooks et tableaux de bord

Microsoft fournit des **Workbooks prédéfinis** dans le portail Entra ID et dans Sentinel pour visualiser la posture de sécurité identitaire. Les tableaux de bord essentiels à surveiller quotidiennement :

- **Sign-in failure analysis** : volume et motifs des échecs d'authentification. Un pic soudain d'échecs "Invalid password" peut indiquer un password spray en cours.
- **Conditional Access insights** : nombre de connexions bloquées par politique, connexions en report-only qui auraient été bloquées, méthodes MFA les plus utilisées.
- **Risky users / Risky sign-ins** : tableau de bord Identity Protection avec les comptes à risque nécessitant une investigation ou une remédiation.
- **Application consent audit** : historique des consentements accordés aux applications, avec focus sur les consentements admin-wide et les applications à permissions élevées (Mail.ReadWrite, Directory.ReadWrite.All, etc.).

8. Checklist de durcissement : 20 points essentiels

Cette checklist synthétise les 20 contrôles de sécurité les plus importants pour durcir un tenant Entra ID. Chaque point est classé par priorité (P1 = critique, P2 = important, P3 = recommandé) et par effort de mise en oeuvre.

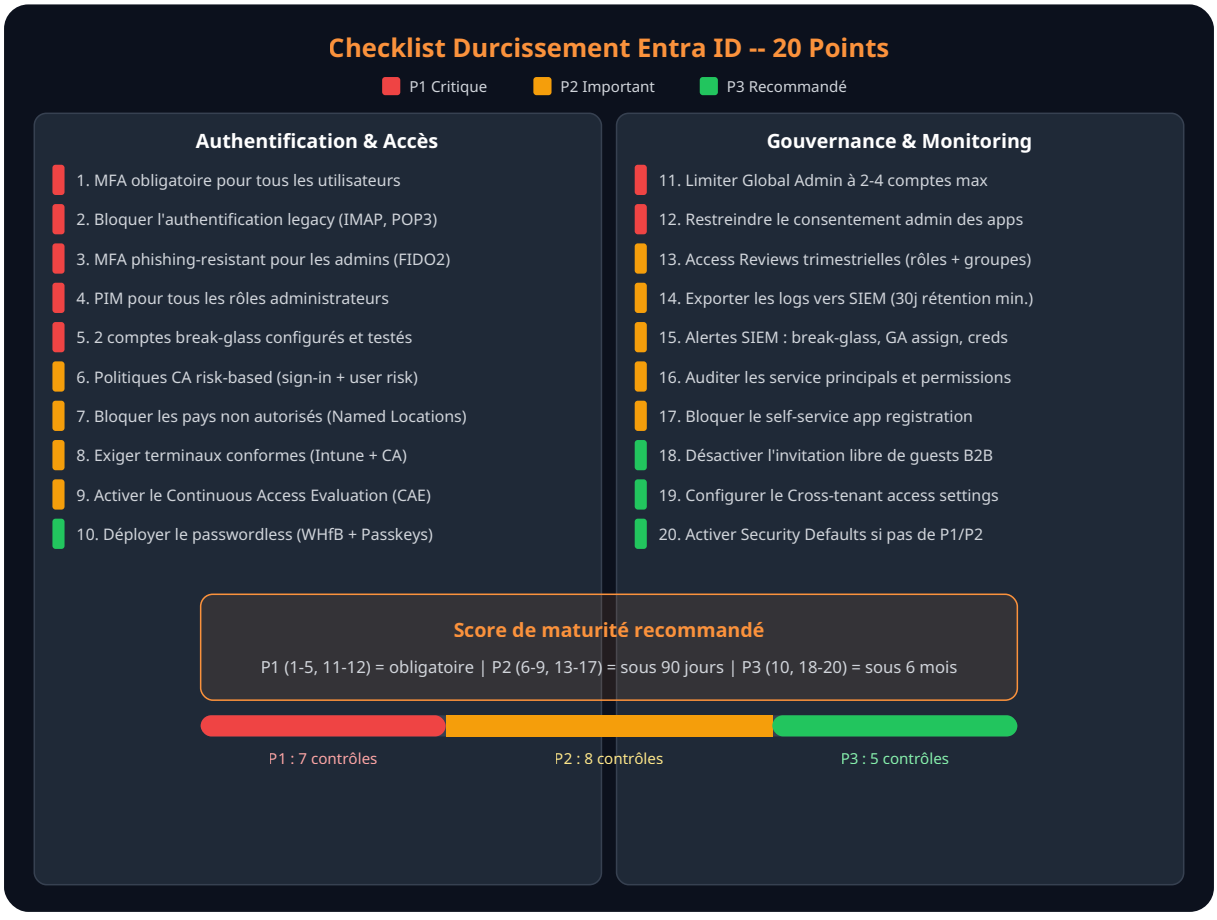

Figure 3 -- Checklist de durcissement Entra ID : 20 points classés par priorité

Détaillons les points les plus fréquemment manqués lors de nos audits :

Gestion des identités Entra ID

Point 5 : comptes break-glass
Plus de 40 % des organisations que nous auditons n'ont pas de procédure break-glass documentée et testée. En cas de panne d'Entra ID, de corruption des politiques CA, ou de compromission des comptes admins, l'absence de break-glass peut entraîner un verrouillage total du tenant -- un scénario catastrophique qui peut prendre des jours à résoudre avec le support Microsoft.

Point 12 : consentement des applications
Par défaut, les utilisateurs peuvent consentir à des applications OAuth demandant des permissions déléguées à faible impact. Cependant, le **consent phishing** exploite cette capacité pour obtenir un accès persistant aux boîtes mail et fichiers. La recommandation : configurer un **Admin Consent Workflow** qui redirige toutes les demandes de consentement vers une équipe d'approbation, tout en maintenant une liste d'applications pré-approuvées pour minimiser la friction.

Point 16 : audit des service principals
Les service principals sont le point aveugle numéro un de la plupart des tenants. Un tenant M365 typique contient des centaines de service principals, dont beaucoup avec des permissions excessives (Directory.ReadWrite.All, Mail.ReadWrite) accordées il y a des mois ou des années et jamais revues. Chaque service principal avec un secret ou un certificat est un vecteur d'accès potentiel qui ne nécessite pas de MFA. Planifiez un audit complet avec `Get-MgServicePrincipal` et `Get-MgServicePrincipalAppRoleAssignment`.

Point 17 : self-service app registration
Par défaut, tout utilisateur peut enregistrer des applications dans le tenant. Cela signifie qu'un utilisateur compromis peut créer une application, lui ajouter des credentials, et l'utiliser comme backdoor persistante. Désactivez cette capacité via `Users can register applications = No` dans les User Settings, et déléguez la création d'applications à un rôle dédié (Application Developer).

Pour approfondir ce sujet, consultez notre outil open-source exchange-security-checker qui facilite la vérification de la sécurité Exchange Online.

Questions frequentes

Comment mettre en place Sécuriser Microsoft Entra ID dans un environnement de production ?

La mise en place de Sécuriser Microsoft Entra ID en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Pourquoi Sécuriser Microsoft Entra ID est-il essentiel pour la securite des systemes d'information ?

Sécuriser Microsoft Entra ID constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

Comment auditer la configuration de sécurité de Sécuriser Microsoft Entra ID : Conditional Access, MFA ?

Utilisez Microsoft Secure Score comme point de départ, puis complétez avec un audit CIS Benchmark pour Microsoft 365. Exportez la configuration via PowerShell pour une revue hors ligne.

Sources et références : Microsoft Security Docs · CERT-FR

> Points clés à retenir
>
> - 8. Checklist de durcissement : 20 points essentiels
> - Gestion des identités Entra ID
> - Questions frequentes
> - 9. Conclusion : la sécurité identitaire comme programme continu

9. Conclusion : la sécurité identitaire comme programme continu

La sécurisation de Microsoft Entra ID n'est pas un projet ponctuel avec une date de fin -- c'est un **programme continu** qui doit évoluer au rythme des menaces et des fonctionnalités. Les attaquants adaptent constamment leurs techniques : le password spraying cède la place au AitM phishing, le vol de mots de passe se transforme en vol de tokens, les attaques manuelles deviennent des campagnes automatisées alimentées par l'IA.

Les organisations qui réussissent leur posture de sécurité identitaire partagent trois caractéristiques :

1. **Une approche layered** : elles ne comptent pas sur un seul contrôle mais sur la combinaison Conditional Access + MFA phishing-resistant + Identity Protection + PIM + monitoring. Chaque couche compense les faiblesses potentielles des autres.
2. **Une gouvernance active** : les Access Reviews sont réellement effectuées, les alertes SIEM sont investiguées, les politiques CA sont régulièrement révisées. La dette technique de sécurité est traitée avec la même rigueur que la dette technique applicative.
3. **Une culture de la sécurité** : les utilisateurs comprennent pourquoi le MFA est nécessaire, les administrateurs savent utiliser PIM, et le RSSI a la visibilité et le soutien de la direction pour implémenter les contrôles nécessaires.

En implémentant les 20 points de la checklist présentée dans cet article, et en s'appuyant sur les mécanismes de détection et de réponse automatique d'Identity Protection, votre organisation sera significativement mieux protégée contre les 80 % de compromissions qui passent par l'identité. Le chemin vers le Zero Trust commence ici -- par la maîtrise de votre plan de contrôle identitaire.

Articles connexes

Identité & Cloud
Sécurité des applications enregistrées Azure AD
Service principals, permissions API, consent phishing
Identité & Attaques
Attaques sur les Identity Providers (Okta, Entra, Keycloak)
Golden SAML, token theft, session hijacking
Authentification
Contournement FIDO2 et Passkeys
Limites du phishing-resistant MFA, attaques device
Protocoles
Sécurité OAuth 2.0 et OpenID Connect
Flows, token security, redirect URI attacks
Social Engineering
Phishing sans pièce jointe : AitM, device code, QR
Techniques modernes de phishing ciblant le MFA
Attaques Credentials
Password Attacks : Cracking, Spraying, Credential Stuffing
Techniques et détection des attaques par mots de passe

Références et ressources externes

- Microsoft Learn -- Conditional Access -- Documentation officielle Conditional Access
- Microsoft Learn -- Identity Protection -- Détection et remédiation des risques identité
- Microsoft Learn -- Privileged Identity Management -- Just-in-time access pour les rôles admin
- MITRE ATT&CK T1078 -- Valid Accounts -- Techniques d'exploitation de comptes valides
- Microsoft Digital Defense Report 2025 -- Rapport annuel sur les menaces Microsoft

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr