



Best Practices WatchGuard AuthPoint - Integration in Microsoft Azure

Thomas Fleischmann

Senior Sales Engineer Central Europe

Thomas.Fleischmann@watchguard.com

Agenda

- Weshalb ist MFA bei Cloud-Diensten wichtig?
- Einrichtung von WatchGuard AuthPoint in Zusammenspiel mit Microsoft Azure
- Was geht, was geht nicht ...
- Demo



Weshalb ist MFA bei Cloud-Diensten wichtig?

Weshalb ist MFA bei Cloud-Diensten wichtig?

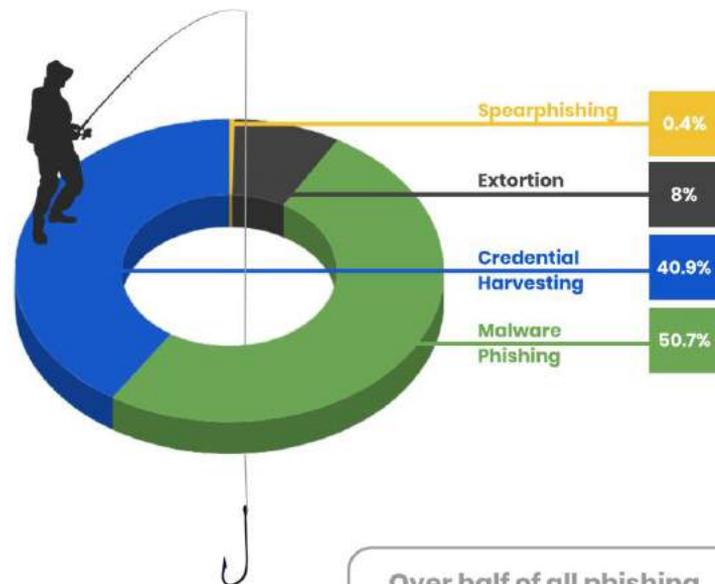
- Microsoft und andere Cloud Provider bieten ihren Kunden die Möglichkeit sich per Username und Passwort an ihre Dienste anzumelden.
- Diese Dienste sind Webseiten, wie z.B. Office365, Google G Suite, AWS Management Console, ...
- Diese Dienste werden nicht von der lokalen Sicherheit des Kunden geschützt.



Weshalb ist MFA bei Cloud-Diensten wichtig?

Phishing

- Viele Phishing Angriffe, die gegen Cloud-Dienste gezielt sind, verbreiten Malware über eingefügte Links, aber etwa die Hälfte der Angriffe zielt darauf ab, Zugangsdaten zu erbeuten.
- Tatsächlich ist Microsoft die am meisten betroffene Unternehmen der Welt, wobei 1 von 3 Angriffen auf Accounts von MS abzielen.



Over half of all phishing attacks contain malware.

2019 Global Phish Report - Avanan

Weshalb ist MFA bei Cloud-Diensten wichtig?

Brute Force Attacken

- Laut Microsoft gibt es jeden Tag mehr als 300 Millionen betrügerische Anmeldeversuche.
- Microsoft hat ein Tool, um diese Angriffe zu simulieren: „Angriffssimulator in Office 365 ATP”
<https://docs.microsoft.com/de-de/microsoft-365/security/office-365-security/attack-simulator>
- Ein Passwortspray-Angriff kann definiert werden als der Versuch, mit einer kleinen Anzahl häufig verwendeter Passwörter auf eine große Anzahl von Benutzerkonten zuzugreifen.
- Ein traditioneller Brute-Force-Angriff verwendet viele Tausende von Passwörtern, um ein oder wenige Benutzerkonten zu knacken.

Weshalb ist MFA bei Cloud-Diensten wichtig?

- *"Microsoft is the number one phished brand for the fourth straight quarter—thanks to Office 365. A multisystem platform, Office 365 combines email, file storage, collaboration, and productivity applications, including OneDrive and SharePoint. Together, they represent a honeypot of sensitive data and files that phishers are looking to exploit."* (Zitat: Vade Secure)

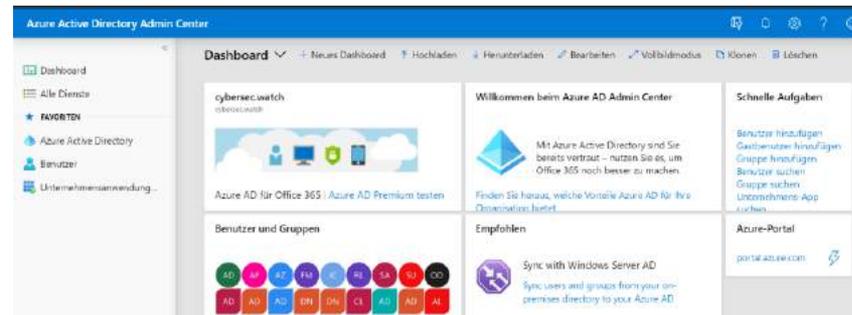




Einrichtung von WatchGuard AuthPoint in Zusammenspiel mit Microsoft Azure

Einrichtung

- Voraussetzung:
 - Microsoft Azure Account
 - WatchGuard Cloud Account mit WatchGuard AuthPoint Lizenzen



Einrichtung

- Anmelden an Azure Portal
 - <https://portal.azure.com/>
- In Bereich Azure Directory den Menü Punkt „App-Registrierungen“ aufrufen.

Dashboard > cybersec.watch | App-Registrierungen > Anwendung registrieren

Anwendung registrieren

Einrichtung

Anwendung registrieren

* Name

Der dem Benutzer gezeigte Anzeigename für diese Anwendung. (Dieser kann später geändert werden.)

Unterstützte Kontotypen

Wer kann diese Anwendung verwenden oder auf diese API zugreifen?

- Nur Konten in diesem Organisationsverzeichnis (nur "cybersec.watch" – einzelner Mandant)
- Konten in einem beliebigen Organisationsverzeichnis (beliebiges Azure AD-Verzeichnis – mehrinstanzenfähig)
- Konten in einem beliebigen Organisationsverzeichnis (beliebiges Azure AD-Verzeichnis – mehrinstanzenfähig) und persönliche Microsoft-Konten (z. B. Skype, Xbox)

[Entscheidungshilfe...](#)

Umleitungs-URI (optional)

Die Authentifizierungsantwort wird nach erfolgreicher Authentifizierung des Benutzers an diesen URI zurückgegeben. Die Angabe ist zum jetzigen Zeitpunkt optional und kann später geändert werden. Für die meisten Authentifizierungsszenarien ist jedoch ein Wert erforderlich.

Web	Beispiel: https://myapp.com/auth
-----	----------------------------------

Indem Sie den Vorgang fortsetzen, stimmen Sie den Microsoft-Plattformrichtlinien zu. [?](#)

Registrieren

Einrichtung

- Wählen Sie unter „Unterstützte Kontotypen“ die Arten von Benutzerkonten aus, die diese Anwendung zur Anmeldung verwenden können.
 - Ihre Auswahl sollte die Benutzer umfassen, die mit WatchGuard AuthPoint synchronisiert wurden oder werden.
- Klicken Sie auf „Registrieren“.
- Eine Seite wird angezeigt, die die Details für Ihre Anwendung enthält. Kopieren Sie den Wert der Anwendungs-(Client-)ID.
 - Sie benötigen diesen Wert, um die externe Identität von Azure AD in AuthPoint zu erstellen.

Anwendungs-ID (Client)

636e4f27-955c-4ed6-866a-f50f29322541

Verzeichnis-ID (Mandant)

3f5c321d-8688-46b8-b25d-cbd0b2472655

Objekt-ID

ff38100e-5c76-46ea-9203-c7a6159ad3b9

Einrichtung

- Im Navigationsmenü „Manifest“ setzen Sie im Manifest-Editor die „allowPublicClient-Eigenschaft“ auf „true“.

 Branding	4	<code>"accessTokenAcceptedVersion": null,</code>
 Authentifizierung	5	<code>"addIns": [],</code>
 Zertifikate & Geheimnisse	6	<code>"allowPublicClient": true,</code>
 Tokenkonfiguration (Vorschau)	7	<code>"appId": "636e4f27-955c-4ed6-866a-f50f29322541",</code>
 API-Berechtigungen	8	<code>"appRoles": [],</code>
 Eine API verfügbar machen	9	<code>"oauth2AllowUrlPathMatching": false,</code>
 Besitzer	10	<code>"createdDateTime": "2019-12-20T07:16:57Z",</code>
 Rollen und Administratoren (Vo...	11	<code>"groupMembershipClaims": null,</code>
 Manifest	12	<code>"identifierUris": [],</code>
	13	<code>"informationalUrls": {</code>
	14	<code> "termsOfService": null,</code>
	15	<code> "support": null,</code>
	16	<code> "privacy": null,</code>
	17	<code> "marketing": null</code>
	18	<code>},</code>

- Klicken Sie auf Speichern.

Einrichtung

- Wählen Sie im Navigationsmenü die Option „API-Berechtigungen“.
- Klicken Sie auf „Berechtigung hinzufügen“.
- Wählen Sie „Microsoft Graph“.

API-Berechtigungen anfordern

Hiermit wählen Sie eine API aus.

Microsoft-APIs Von meiner Organisation verwendete APIs Eigene APIs

Häufig verwendete Microsoft-APIs



Microsoft Graph

Nutzen Sie die gewaltige Datenmenge in Office 365, Enterprise Mobility + Security und Windows 10. Greifen Sie auf Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planer und vieles mehr über einen einzigen Endpunkt zu.

Einrichtung

- Wählen Sie „Anwendungsberechtigungen“.

API-Berechtigungen anfordern

< Alle APIs



Microsoft Graph

<https://graph.microsoft.com/> [Dokumente](#)

Welche Art von Berechtigungen sind für Ihre Anwendung erforderlich?

Delegierte Berechtigungen

Ihre Anwendung muss als der angemeldete Benutzer auf die API zugreifen.

Anwendungsberechtigungen

Ihre Anwendung wird als Hintergrunddienst oder Dämon ohne angemeldeten Benutzer ausgeführt.

- Wählen Sie die „Anwendungsberechtigungen“
 - Group.Read.All** und **User.Read.All**

Group (1)

<input type="checkbox"/>	Group.Create Create groups ⓘ	Ja
<input checked="" type="checkbox"/>	Group.Read.All Read all groups ⓘ	Ja
<input type="checkbox"/>	Group.ReadWrite.All Read and write all groups ⓘ	Ja
<input type="checkbox"/>	Group.Selected Access selected groups ⓘ	Ja

User (1)

<input type="checkbox"/>	User.Export.All Export user's data ⓘ	Ja
<input type="checkbox"/>	User.Invite.All Invite guest users to the organization ⓘ	Ja
<input type="checkbox"/>	User.ManageIdentities.All Manage all users' identities ⓘ	Ja
<input checked="" type="checkbox"/>	User.Read.All Read all users' full profiles ⓘ	Ja
<input type="checkbox"/>	User.ReadWrite.All Read and write all users' full profiles ⓘ	Ja

Einrichtung

- Wählen Sie „Delegierte Berechtigungen“.
- Wählen Sie die Berechtigung **User.Read**.

> Contacts

▼ DelegatedPermissionGrant (1)



DelegatedPermissionGrant.ReadWrite.All
Manage all delegated permission grants ⓘ

Ja

> Device

- Klicken Sie auf Berechtigungen hinzufügen.
- Die hinzugefügten Berechtigungen müssen vom Administrator genehmigt werden!

Einrichtung

- Wählen Sie im Navigationsmenü „Zertifikate und Geheimnisse“.
- Klicken Sie auf „Geheime Clientschlüssel“.
- Wählen sie ein Enddatum für die Gültigkeit des Schlüssels aus.
- Klicken Sie auf „Hinzufügen“.
- Details des neuen „Geheime Clientschlüssel“ werden angezeigt.
- Kopieren Sie den „Geheime Clientschlüssel“. Sie benötigen diesen Wert, um die „Externe Identität“ von Azure AD in WatchGuard AuthPoint zu erstellen.

Geheime Clientschlüssel

Eine geheime Zeichenfolge, die von der Anwendung beim Anfordern eines Tokens als Identitätsnachweis verwendet wird. Wird auch als Anwendungskennwort bezeichnet.

+ Neuer geheimer Clientschlüssel

Beschreibung	Gültig bis	Wert
AuthPoint	20.12.2021	:h@*****

Einrichten

- Einrichten einer „External Identities“ für Azure AD.
- Unter „External Identities“ den Wert „Azure AD“ auswählen.



- Im folgenden Menü muß die Application ID und Clientschlüssel eingetragen werden.

Einrichten

Azure AD

Enable

Name *

Application ID *

Domain *

To change your Client Secret, fill out the field below.

Client Secret *

Synchronization Interval *



Einrichten

- Prüfen der Verbindung zur Azure AD

Cybersec.watch AD	Azure AD
fmann.local	Ldap

Cybersec.watch AD

- Group Sync
- Start Synchronization
- Check Connection
- Delete

Einrichten

- Synchronisieren Sie Ihre Benutzer
- Nachdem Sie eine „External Identities“ für Ihren Azure AD erstellt haben, müssen Sie eine Gruppensynchronisation hinzufügen.
 - Die Azure AD-Gruppen zur Synchronisierung von Benutzern
 - Die AuthPoint-Gruppe zum Hinzufügen der Benutzer

Update Azure AD Group Sync ×

Select Azure AD Groups *

CLOUD-SICHERHEIT-MIT-MFA ×

Select Azure AD Groups

Select the AuthPoint Group *

Cloud Sicherheit ▾

CANCEL SAVE



Was geht, was geht nicht ...

Was geht, was geht nicht ...

- Folgende Herausforderung existiert noch
 - Reine Azure AD / Office365 Benutzer und MFA
- Es werden keine neuen 3rd Party MFA Provider von Microsoft zertifiziert.
- Nur durch eine Freigabe von Microsoft kann man somit reine Azure AD User mit MFA verbinden.
- Folge ist, daß WatchGuard AuthPoint nur in einer Hybrid AD die Azure AD User integrieren kann. Des Weiteren kann man MFA für Office 365 User mit einer ADFS Integration abbilden.

(<https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/AuthPoint/Office365-AuthPoint.html>)



Demo



THANK YOU