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?

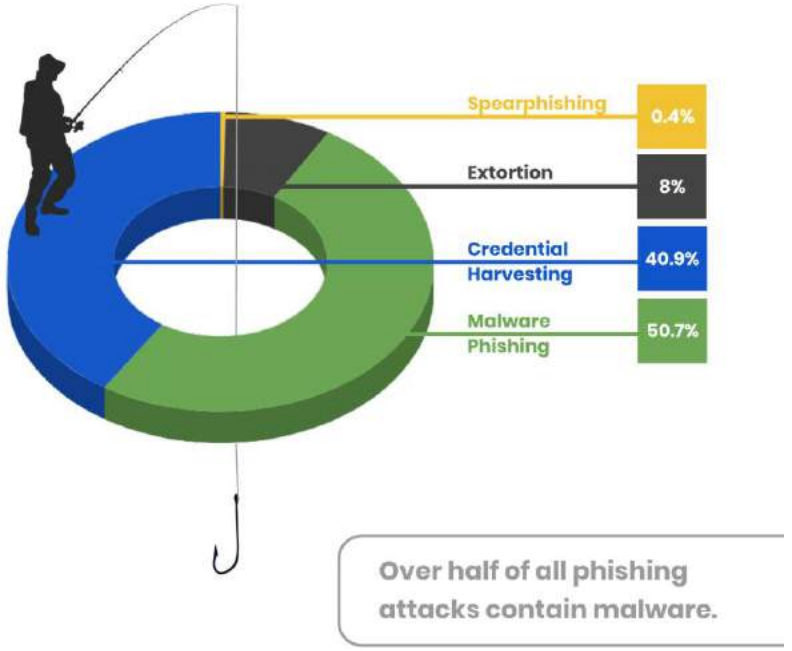
- Microsoft und andere Cloud Provider bieten ihren Kunden die Möglichkeit sich per Username und Passwort an ihre Dienste anzumelden.
- Diese Dienste sind Webseiten, wie z.B. Office365, Google G Suite, AWS Management Console, …

- Diese Dienste werden nicht von der lokalen Sicherheit des Kunden geschützt.

Weshalb ist MFA bei Cloud-Diensten wichtig?

Phishing

- Viele Phishing Angriff, 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 Unter-nehmen der Welt, wobei 1 von 3 Angriffen auf Accounts von MS abzielen.



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.

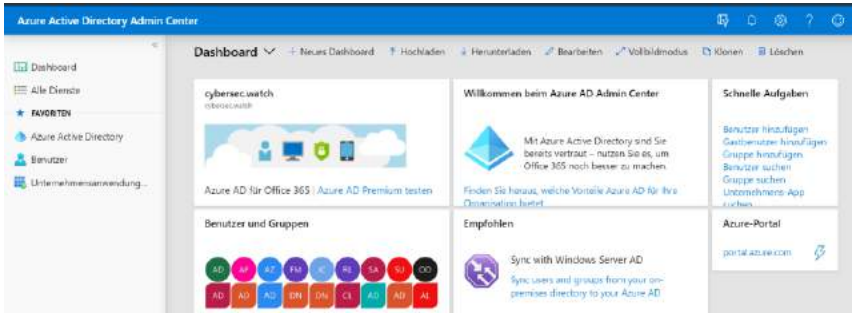
Weshalb ist MFA bei Cloud-Diensten wichtig?

- *"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

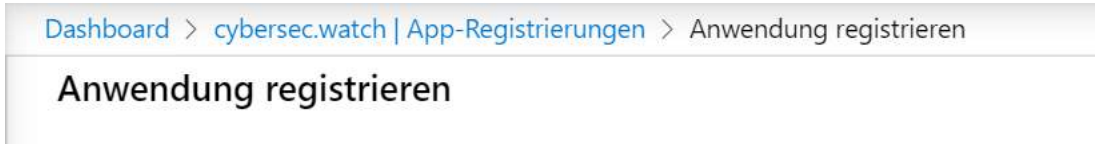
- Voraussetzung:
  - Microsoft Azure Account
  - WatchGuard Cloud Account mit WatchGuard AuthPoint Lizenzen



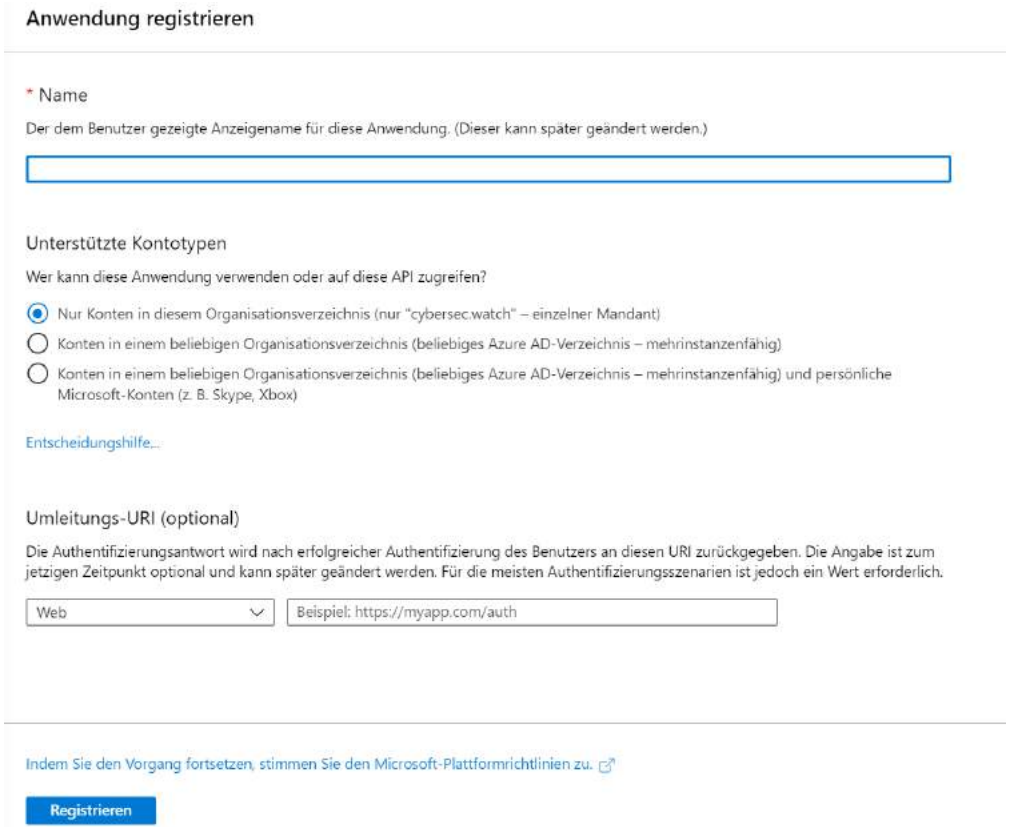
Einrichtung

- Anmelden an Azure Portal
  - https://portal.azure.com/

- In Bereich Azure Directory den Menü Punkt „App-Registrierungen“ aufrufen.



Einrichtung

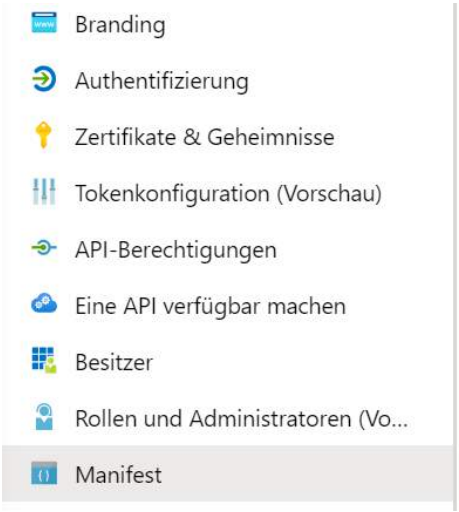


Einrichtung

- 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.

Einrichtung

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



- Klicken Sie auf Speichern.

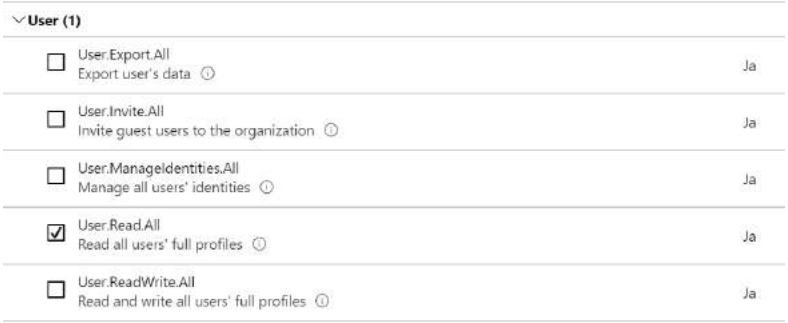
Einrichtung

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

Einrichtung

- Wählen Sie „Anwendungsberechtigungen“.

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



Einrichtung

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

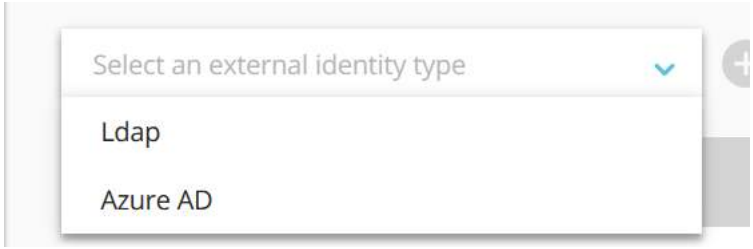
- Klicken Sie auf Berechtigungen hinzufügen.
- Die hinzugefügten Berechtigungen müssen vom Administrator genehmigt werden!

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.

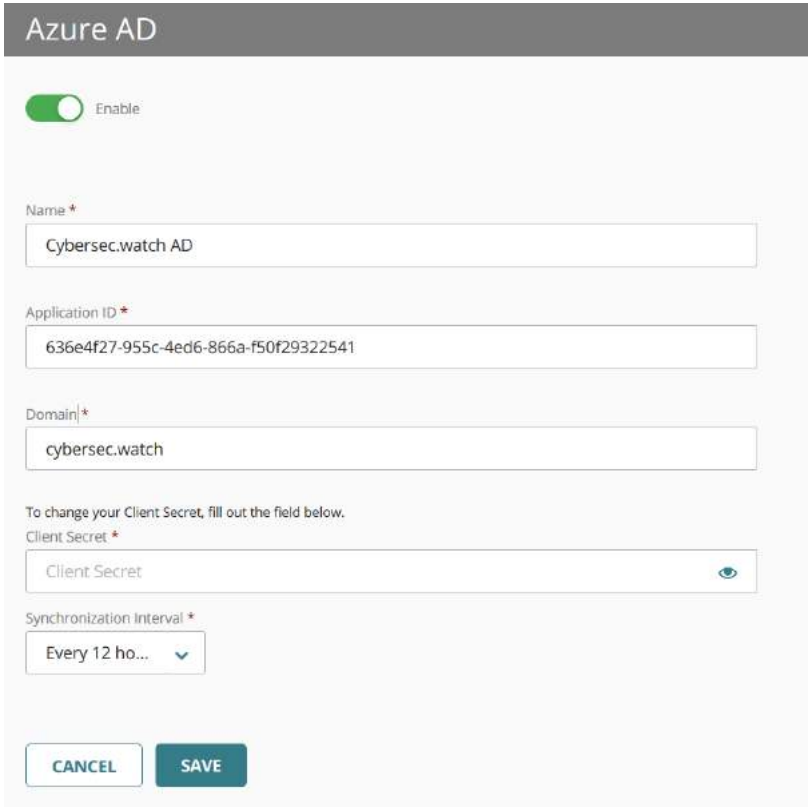
Einrichten

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



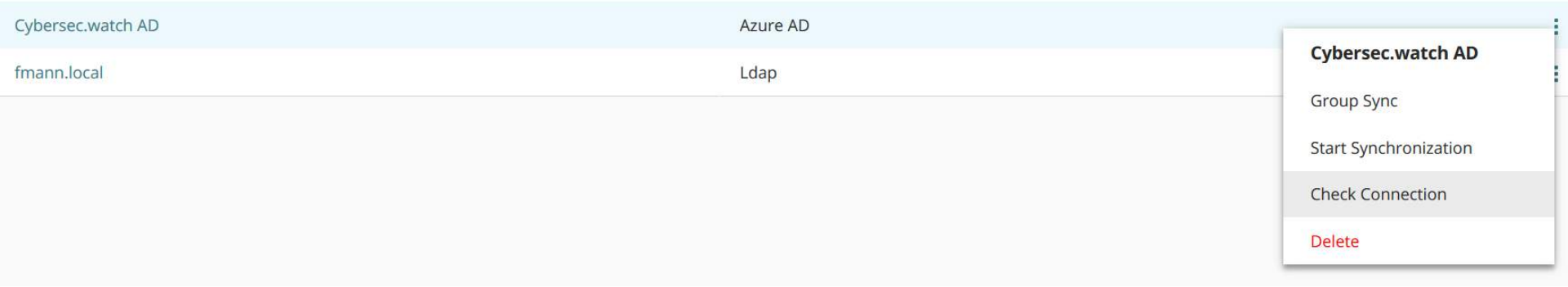
- Im folgenden Menü muß die Application ID und Clientschlüssel eingetragen werden.

Einrichten



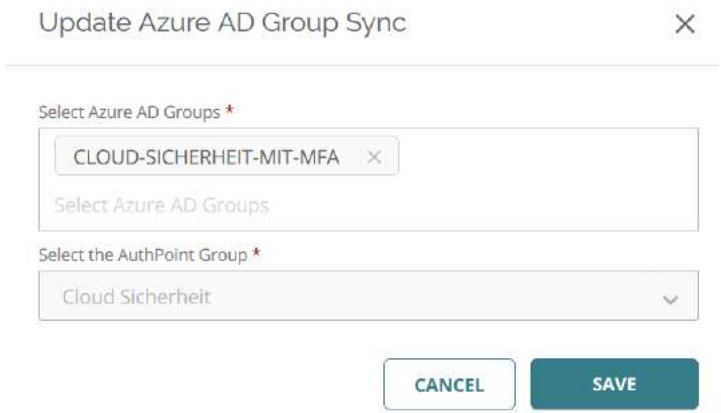
Einrichten

- Prüfen der Verbindung zur Azure AD



Einrichten

- Synchronisieren Sie Ihre Benutzer
- Nachdem Sie eine „External Identies“ 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



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)