

Best Practice – AuthPoint Integration von ADFS Ressourcen



Der Verlust eines Kennworts ist schnell passiert!

Selbst mit bestens aufgestellter Perimeter- und Endgerätesicherheit ist es schnell passiert:

1 Benutzerkennwort wird gehackt • 1 Computer ist mit einem Keylogger infiziert •

• 1 Nutzer teilt seinen Pin mit



... und der Angreifer hat vollen Zugriff, fast als würde er vor Ort im Unternehmen sein



MFA schützt mit mehr als nur einem Passwort



Multi-Faktor-Authentifizierung ist ein wesentlicher Schutz

Durch die Anforderung eines zusätzlichen Identitätsnachweises über ein einfaches Passwort hinaus ist die Multi-Faktor-Authentifizierung (MFA) die wichtigste Schutzmaßnahme zum Schutz Ihres Unternehmens hGuard



AuthPoint schützt VPNs, Web Apps, PC-Anmeldung und mehr!







ADFS Integration



Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved

Was ist eigentlich ADFS?

- Microsoft Active Directory Federation Services ist eine Plattform zur sicheren Anmeldung an internen und externen Systemen.
 - Das System basiert auf einem Web Service, der die Anwender am Active Directory authentifiziert und parallel den Zugriff auf "Claims-Aware" Applikationen ermöglicht (z.B. Office 365, Salesforce.com, etc.).
 - Diese Applikationen können on-premise, off-premise oder sogar bei anderen Firmen installiert sein. Es ist nahezu unerheblich "wo" die Anwendung installiert ist, solange der ADFS Standard unterstützt wird.



Grundlegender Aufbau von ADFS?









z.B. Office 365 mit on-premise AD und ADFS mit AuthPoint





Office365 – Warum nicht SAML?

- Guide zu AuthPoint mit Office365 per SAML: <u>https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/AuthPoint/Office365-AuthPoint.html</u>
- SAML erfordert keine Installation des ADFS Gateway und benötigt weniger Konfigurationsschritte
- SAML ist weniger flexibel
 - Bei SAML müssen alle Nutzer AuthPoint verwenden, mit ADFS können Ausnahmen über AD Gruppe umgesetzt werden.
 (Bei SAML ist eine Ausnahme von der Anwendung von MFA zwar möglich, aber jeder Nutzer benötigt eine AuthPoint Lizenz)



Anforderungen

- Vorhandenes Active Directory als Benutzerdatenbank
- ADFS Installation auf Windows Server
- Applikation, die ADFS verwendet (z.B. interne Web-Applikation oder Office365)
- Integration von WatchGuard AuthPoint
- (spezifische) Anwender müssen nun MFA nutzen





Aktivieren von ADFS in AuthPoint

Hinzufügen einer neuen Ressource

WatchGuard	Dashboard	Monitor	Configure	Administration	Ŷ	8	0	
AuthPoint	ADF	S						
Summary	Name *							
Management	My E	My Example AD FS						
Resources								
Groups			AVE					
Users								
External Identities								
Gateway								



Aktivieren von ADFS in AuthPoint

Hinzufügen der Ressource zu eine AuthPoint Gateway

WatchGuard	Dashboard Monitor	Configure	Administration				Ŷ	?	9		
AuthPoint	Add Gateway								Q		
Summary	NAME		^	VERSION							
Management Resources	Test Gateway x.x.x-xxx							-			
Groups Users	ADFS										
External Identities							22				
Gateway	Select an ADFS resource										
	Select an ADFS										
	My Example AD FS										
	LDAP										
(#	Select an LDAP external identity	r.					12				
	Select a LDAP										



Installation ADFS Agent

- Die Installationsdatei findet sich in AuthPoint im Bereich Downloads.
- Eine ADFS Ressource muss bereits vorhanden sein. Das AuthPoint Gateway muss Version 4.0.0 oder höher sein, damit auch die erforderliche Konfigurationsdatei des ADFS Agent verfügbar ist.
- Mit Download Config kann nun die Konfigurationsdatei heruntergeladen werden. Sind mehrere AuthPoint Gateways verfügbar kann ausgewählt werden welches Gateway mit der ADFS Funktion genutzt werden soll.
- Die Installationsdatei und die Konfigurationsdatei können nun in den gleichen Ordner auf dem ADFS server kopiert werden.
- Installation starten







15

Copyright ©2019 WatchGuard Technologies, Inc. All Rights Reserved













Anmeldung mit AuthPoint







Live Demo



20



Vielen Dank!



NOTHING GETS PAST RED.



