TRAININGSKURS

OXFORD COMPUTER GROUP

AZURE AD Identity and Security Training

Kurscode A630

Kursbeschreibung

Dieser sehr praxisorientierte Azure AD Identity and Security-Trainingskurs beinhaltet umfassend und tiefgehend die wichtigsten Azure Identitäts- und Anwendungssicherheitsfunktionen. Er gibt den Teilnehmern die Möglichkeit, eine starke Identitäts- und Anwendungszugriffslösung in Azure mit Zero Trust als Herzstück implementieren zu können.

Für wen ist dieser Trainingskurs gedacht?

Diese 4-tägige Azure AD Identity and Security-Schulung richtet sich an IT-Support-Mitarbeiter, IT-Berater und -Architekten, Pre-Sales-Mitarbeiter, technisch versierte Entscheider und Abteilungsleiter, die wissen wollen:

- Wie man Azure AD Connect konfiguriert und implementiert, um lokale Benutzer und Gruppen mit Azure AD zu synchronisieren - zusammen mit den Authentifizierungsoptionen.
- Wie man SaaS-Anwendungen und lokale Anwendungen sicher integriert.
- Wie Sie die Self-Service-Passwortrücksetzung und die Self-Service-Gruppenverwaltung implementieren.
- Wie man Conditional Access (sowohl für Cloud-Apps als auch für on-premises-Apps) konfiguriert, um Benutzeranfragen zu bewerten und die Multi-Faktor-Authentifizierung (MFA) auf Basis von Faktoren wie Identität, Risikostufe und Standort des Benutzers zuzulassen, zu verweigern oder zu erzwingen.
- Wie Sie Benutzerrisiken auf der Basis von publik gewordenen Anmeldeinformationen, Verhaltensanalysen o.ä. überwachen.
- Wie automatische Abhilfemaßnahmen wie Erzwingen von MFA oder Zurücksetzen des Passworts eingerichtet werden.
- Wie Sie den Zugriff auf privilegierte Rollen beschränken können.

Dieser sehr praxisorientierte Kurs umfasst Präsentationen, Diskussionen, Demonstrationen und über 50 praktische Übungen!

Diese Übungen - die für das richtige Verständnis der behandelten Themen entscheidend sind - wurden so realistisch wie möglich gestaltet. Sie sind komplex und spiegeln Probleme wider, die Sie in der realen Welt antreffen und beheben müssen. So werden die Teilnehmer zum Beispiel eine echte Domain kaufen und EM+S/O365 mit öffentlichen E-Mails und echten Zertifikaten für Single Sign-on vollständig implementieren. Die Teilnehmer können diese Sandbox-Umgebung für die spätere Verwendung behalten.

Am Ende des Kurses werden die Teilnehmer in der Lage sein:

- die Synchronisierung von on-premises AD-Informationen mit Azure AD unter Verwendung von Azure AD Connect, einschließlich Benutzern und Gruppen, mit Authentifizierungsoptionen durchzuführen.
- Azure AD Connect zu überwachen.
- Lizenzen direkt und über Gruppen (Cloud und on-premises) zuzuweisen.
- verschiedene Self-Service-Funktionen wie Self-Service-Passwortregistrierung, Self-Service-Passwortrücksetzung, Self-Service-Gruppenverwaltung und Self-Service-Anwendungsverwaltung zu konfigurieren.
- Cloud-MFA zu implementieren und dieses für die Step-up-Authentifizierung für sensible Anwendungen zu nutzen und Key Accounts zu schützen.

Oxford Computer Group GmbH
Gießereistraße 16
85435 Erding
Deutschland

T +49 81 22 89 20 89-0
F +49 81 22 89 20 89-99
E info@ocg.de
I www.ocg.de

Gold Microsoft Partner
Microsoft

TRAININGSKURS

OXFORD COMPUTER GROUP

AZURE AD Identity and Security Training

Kurscode A630

- lokale Anwendungen sicher in der Cloud zu veröffentlichen.
- SaaS-Anwendungen mit Authentifizierung bereitzustellen.
- Identitätssicherheitsfunktionen von Azure AD, wie z.B. Privileged Identity Management und Identitätsschutz zu nutzen.
- eine sehr praxisnahe Umgebung aufzubauen, sodass sie Lösungen testen, implementieren und bereitstellen können.

Bitte beachten Sie:
Ein wesentlicher Bestandteil der Übungsumgebung ist, dass sie über eine echte Domäne und echte Zertifikate sowie eine echte Microsoft Azure-Testversion verfügt. Um dies zu ermöglichen, müssen die Teilnehmer eine Kreditkarte bereitstellen. Normalerweise werden die Gesamtkosten 30 € nicht überschreiten.

> **Dieser Kurs ist als öffentlicher Kurs verfügbar, entweder vor Ort in Erding oder online über Teams. Alternativ auch als Inhouse Schulung.**

Nachfolgend finden Sie alle Details zu den Trainingsinhalten:

Die Teilnehmer dieses sehr praxisorientierten Kurses erhalten eine solide Grundlage in den wichtigsten Identitäts- und Sicherheitsfunktionen in Azure AD, die für Microsofts Zero Trust Strategie („never assume trust, always verify") von zentraler Bedeutung sind. Der Kurs beinhaltet Vorträge, Diskussionen und detaillierte praktische Übungen.

Wir bieten detaillierte Schritt-für-Schritt-Anleitungen für die Übungen. Die Teilnehmerzahl ist begrenzt, so dass Ihr Dozent genügend Zeit hat, Ihnen bei Problemen in den Übungen zu helfen und alle Fragen zu beantworten.

Die praktischen Übungen sind entscheidend für das richtige Verständnis der behandelten Themen und wurden so realistisch wie möglich gestaltet.

In diesem Sinne werden die Teilnehmer ihre eigene Azure/O365-Umgebung vollständig implementieren und eine echte Domain mit öffentlichen E-Mails und einem echten Zertifikat für Single Sign-On (SSO) erwerben.

Über vier volle und arbeitsreiche Tage hinweg werden Sie ein tiefes und praktisches Verständnis erlangen von:

Modul 1: Azure Cloud Computing

In diesem Modul stellen wir Cloud Computing vor und veranschaulichen, wie es in Azure durch den Einsatz verschiedener Technologien, wie virtuelle Maschinen, Cloud-Dienste, Cloud-Lizenzen und die Azure AD-Identity Plattform, implementiert werden kann.

Modul 2: AD und Azure AD

In diesem Modul betrachten wir das (lokale) Active Directory und das (Cloud) Azure Active Directory und untersuchen einige der wichtigsten Gemeinsamkeiten und Unterschiede.

In dieser Übungseinheit führen wir Sie durch die Einrichtung eines Azure AD-Tenants mit einem benutzerdefinierten Domänennamen. Anhand unserer Schritt-für-Schritt-Anleitung kaufen Sie einen Domainnamen, richten ein Azure-Testabonnement ein, erstellen einen Azure AD-Tenant und fügen diesem Ihren benutzerdefinierten Domainnamen hinzu. Nachdem Sie Ihren benutzerdefinierten Azure AD-Tenant eingerichtet haben, führen wir Sie durch die Erstellung von Azure Virtual Machines, die in späteren Übungen zur Simulation verschiedener lokaler Maschinen (ein Domain-Controller, ein IIS-Server und ein Proxy-Server) verwendet werden.

Modul 3: Integration von AD und AAD

Hier betrachten wir die Notwendigkeit der Synchronisation und wie Azure AD Connect verwendet werden kann, um Benutzer und Gruppen zwischen AD und Azure AD zu synchronisieren. Dies geschieht in einfachen und komplexeren Multi-Forest-Szenarien. Wir behandeln zahlreiche fortgeschrittene Themen, darunter die Installationsoptionen, die verschiedenen Optionen für die Kennwortsynchronisierung, den Zweck von Synchronisierungsregeln und warum sie möglicherweise geändert werden müssen, sowie die Überwachung von Azure AD Connect.

Oxford Computer Group GmbH
Gießereistraße 16
85435 Erding
Deutschland

T +49 81 22 89 20 89-0
F +49 81 22 89 20 89-99
E info@ocg.de
I www.ocg.de

Gold Microsoft Partner
Microsoft

TRAININGSKURS

OXFORD COMPUTER GROUP

AZURE AD Identity and Security Training

Kurscode A630

In dieser Übung werden Sie Ihr lokales AD mit Benutzern füllen und diese mit Ihrer Azure AD-Instanz synchronisieren. Sie werden dabei verschiedene Azure AD Connect-Funktionen wie OU-Filterung, Regelbearbeitung, Passwortrückschreibung und SSO untersuchen. Sie werden auch das Azure AD Connect-Health Monitoring und dazugehörige Alerts einrichten und konfigurieren.

Es gibt auch eine optionale Übung, die Sie durch die Installation und Konfiguration sowohl eines AD FS-Servers als auch eines Web Application Proxy-Servers führt. Nachdem Sie diese eingerichtet haben, werden Sie Azure/O365 so konfigurieren, dass AD FS für die Authentifizierung verwendet wird. Außerdem können Sie die Erfahrung der Endbenutzer untersuchen.

Modul 4: grundlegende AADP-Verwaltung

In diesem Modul konzentrieren wir uns auf einige der Funktionen, die in einer Azure Active Directory Premium-Lizenz enthalten sind. Zu Beginn besprechen wir die Lizenzzuweisung (direkt an Einzelpersonen und indirekt über Gruppen) und die verschiedenen Verwaltungs- und Benutzeroberflächen. Außerdem behandeln wir die Anpassung Ihres Azure AD-Brandings, die Benutzer- und Gruppenverwaltung und die Integration von SaaS-Apps (und die verschiedenen Integrationsebenen wie Password Vaulting, Federation und eingehende oder ausgehende Benutzerbereitstellung). Schließlich untersuchen wir die Optionen für Audit-Protokolle, Anmelde- und Sicherheitsberichte und besprechen, wie sie analysiert werden können.

In dieser Übungseinheit werden Sie Ihre Azure AD-Anmeldeseite anpassen und mit der direkten und indirekten Zuweisung von Lizenzen experimentieren (zu Gruppen, die aus Ihrem lokalen AD synchronisiert wurden). Sie erkunden die grundlegende UI-Verwaltung und fügen SaaS-Apps hinzu: eine mit konfiguriertem SSO, eine weitere mit aktiviertem Passwort-Vaulting und optional eine dritte SAML-konforme SaaS-App mit aktiviertem Provisioning. In der letzten Übung werden Sie einige der vordefinierten Berichte in Azure überprüfen.

Modul 5: Self-Service

In diesem Modul dreht sich alles um Self-Service: Die Self-Service-Gruppenverwaltungsoptionen zum Erstellen und Beitreten von Gruppen (mit oder ohne Genehmigung des Eigentümers), die Self-Service-Funktionen zum Bereitstellen des Anwendungszugriffs und die Self-Service-Kennwortregistrierung und -zurücksetzung. In der Übung werden Sie alle Aspekte des Self-Service Gruppenmanagements sowohl als Administrator (Aktivierung) als auch als Benutzer (Erstellen von Gruppen und Beantragen des Beitritts zu Gruppen sowie Genehmigen von Mitgliedschaftsanträgen als Gruppenbesitzer) kennenlernen. Anschließend implementieren Sie die Self-Service-Anwendungsverwaltung als Administrator und beantragen den Zugriff (als Benutzer). Abschließend implementieren und testen Sie die Self-Service-Kennwortrücksetzung - sowohl als Administrator als auch als Benutzer.

Modul 6: Andere AADP-Features

In diesem Modul geht es um Cloud MFA und den Azure AD Application Proxy (beides Azure Active Directory Premium Features). Wir behandeln die verschiedenen Möglichkeiten, MFA zu erwerben. Um eine starke Authentifizierung für die Anmeldung an modernen Office-Clients bereitzustellen, betrachten wir die verschiedenen Konfigurationsoptionen für die Implementierung von Cloud MFA und wie diese genutzt werden können. Wir werfen auch einen detaillierten Blick darauf, wie der Azure AD Application Proxy genutzt werden kann, um einen sicheren Zugriff auf on-premises-Anwendungen zu ermöglichen - und zwar von jedem Ort der Welt aus, ohne die Notwendigkeit einer traditionellen VPN-Technologie.

In den Übungen werden Sie Cloud MFA konfigurieren und die Multi-Faktor-Authentifizierung für einige Benutzer erzwingen sowie die Erfahrungen der Endbenutzer testen und vergleichen. In Ihrer Azure AD Application Proxy-Übungsumgebung veröffentlichen Sie eine Anwendung, die auf Ihrem lokalen Webserver (einer Ihrer Azure-VMs) gehostet wird, und testen den Zugriff darauf sowohl von innerhalb als auch von außerhalb Ihres Unternehmensnetzwerks. Die weitere Konfiguration umfasst die Aktivierung von SSO, die Bereitstellung zur Auswahl im Office 365 App-Launcher und die Aktivierung des Self-Service-Zugriffs. Schließlich werden Sie einen benutzerdefinierten Namen für die Anwendung implementieren.

Es gibt auch eine optionale Übung, die die Bereitstellung des Azure Multi-Faktor-Authentifizierungsservers, die Integration mit Ihrem lokalen Active Directory und die Konfiguration von AD FS zur Nutzung für aktive Client-Authentifizierungsanfragen abdeckt.

Oxford Computer Group GmbH
Gießereistraße 16
85435 Erding
Deutschland

T +49 81 22 89 20 89-0
F +49 81 22 89 20 89-99
E info@ocg.de
I www.ocg.de

Gold Microsoft Partner

Microsoft

TRAININGSKURS

OXFORD COMPUTER GROUP

AZURE AD Identity and Security Training

Kurscode A630

Modul 7: Implementieren von bedingtem Zugriff (Conditional Access)

In diesem Modul dreht sich alles um den bedingten Zugriff, der grundlegend für eine Zero Trust-Zugriffskontrollstrategie ist. Wir betrachten, was es ist und wofür es verwendet werden kann. Falls gewünscht, besprechen wir, wie man MFA aufrufen kann und wie die Konfiguration von Richtlinien für den bedingten Zugriff und die damit verbundene Möglichkeit, den Anwendungszugriff zu kontrollieren, möglich ist.

In der Übungseinheit werden Sie identitätsbasierte (Gruppenmitgliedschaft) und standortbasierte (vertrauenswürdige und nicht vertrauenswürdige Netzwerke) Zugriffsberechtigungen für Exchange Online einrichten und testen.

Modul 8: Implementieren von Privileged Identity Management (PIM)

In diesem Modul behandeln wir PIM (Teil eines Zero Trust Least Privilege-Ansatzes) und wie es zur Steuerung, Überwachung, Alarmierung und Überprüfung von administrativen Zugriffsrollen in Azure AD eingesetzt werden kann.

In der Übung werden Sie verschiedenen Benutzern administrative Azure AD-Rollen zuweisen und PIM einrichten und konfigurieren. Nach der Aktivierung werden Sie die Aktivierung und Deaktivierung von PIM-Rollen testen. Sie werden auch PIM-Alerts für administrative Rollen einrichten und eine Überprüfung der privilegierten Zugriffszuweisungen eines Benutzers durchführen.

Modul 9: Implementierung Identity Protection

In diesem Modul besprechen wir den Identitätsschutz, eine weitere zentrale Funktion für jede Zero Trust-Implementierung. Wir gehen dabei auf Risikoereignisse, Risikostufen, Sicherheitsrichtlinien für Benutzerrisiken und Sicherheitsrichtlinien für Anmeldungsrisiken ein und zeigen, wie sich diese Risiken beheben lassen.

In den Übungen werden Sie den Azure AD Identitätsschutz einrichten. Sie installieren einen „Anonymitätsbrowser" und verwenden ihn, um das Azure-Portal zu besuchen - dies erzeugt anonyme IP-Adress-Identitätsschutz-Risikoereignisse, die Sie dann überprüfen und beheben werden.

Schließlich konfigurieren Sie die Identity Protection-Anmelderichtlinie und die Benutzerrisikorichtlinie so, dass bestimmte Ereignisse automatisch entschärft werden können (Sie werden sowohl MFA als auch Kennwortänderungen verwenden) und Sie werden beide Richtlinien testen.

Behalten Sie Ihre Übungsumgebung:

Testabonnements und Lizenzen für Azure AD, Enterprise Mobility + Security und Microsoft 365 (offiziell Office 365) werden während des Kurses verwendet, wobei der „on-premises"-Aspekt der Umgebung mit Azure VMs innerhalb des Azure-Testabonnements implementiert wird. Wenn die Teilnehmer die Umgebung als ihre eigene Sandbox für die zukünftige Nutzung behalten möchten, dann kann das Testabonnement nach dem Kurs in ein Pay-As-You-Go-Abonnement umgewandelt werden. Von den Teilnehmern wird die Angabe einer Kreditkarte benötigt, um die Domain, die Zertifikate und das Probeabonnement zu sichern - dies ist jedoch nur mit geringen Kosten verbunden (ca. 30 €).

" Möchten Sie lernen, wie Sie das Beste aus Azure AD Connect herausholen - dann melden Sie sich für unser Azure AD Connect Masterclass Training an!

Oxford Computer Group GmbH
Gießereistraße 16
85435 Erding
Deutschland

T +49 81 22 89 20 89-0
F +49 81 22 89 20 89-99
E info@ocg.de
I www.ocg.de

Gold Microsoft Partner
Microsoft