



Grundlagen

Microsofts Active Directory ist der am meisten genutzte Verzeichnisdienst weltweit – kein Wunder, lassen sich damit die Ressourcen eines Unternehmens äußerst komfortabel verwalten. Das macht das AD aber auch zu einem beliebten Angriffsziel. Wer verstehen will, wie Cyberkriminelle den zentralen Dienst angreifen und wie man ihn absichert, muss wissen, wie das AD grundlegend funktioniert.

ab Seite 7

Grundlagen

Ressourcenmanagement

Komfortable IT-Schaltzentrale mit Schwachpunkten 8

Strukturüberblick

Ein Verzeichnisdienst für alle(s) 16

Informationsbeschaffung

Was jeder Domänenbenutzer alles sieht 24

Wissenspool

Ausgewählte Quellen und Werkzeuge zur Sicherheit von Active Directory 32

Wörterverzeichnis

Das Active-Directory-Glossar 36

Angriffsszenarien

Passwörter und Hashes

Wie Angreifer die Domäne kompromittieren 42

Berechtigungen

Wie Angreifer sich im Active Directory Zugriff verschaffen 49

Rechtevergabe

Wie Angreifer Tickets, Delegation und Trusts missbrauchen 56

Inter-Forest und Persistenz

Wie Angreifer sich über einen AD-Forest hinaus ausbreiten 64

Zertifikatsmissbrauch

PetitPotam und weitere Wege, die Kontrolle über das Active Directory zu übernehmen 72

Abwehrstrategien

Enterprise Access Model

Active Directory mit dem Schichtenmodell schützen 84

Privilegierte Zugriffe besonders absichern 90

Privilegierte AD-Zugriffe managen 96

Gruppenrichtlinien und mehr

Wie Administratoren ihr Active Directory absichern 102

Selbstaudits

AD-Härtungsmaßnahmen jenseits von Group Policies 108

Incident Response und Forensik

Angreifer durch Logs enttarnen 115

Deception

Wie Angreifer in die Falle gelockt werden 121

Zugangsdaten

Passwortsicherheit (nicht nur) im Active Directory 129

IT-Grundschutz

Active Directory grundschutzkonform absichern 136

Marktübersicht

Tools für die Absicherung des Active Directory 145

IT-Forensik

Angriffsspuren analysieren 154

Azure AD

Grundlagen

Das Azure Active Directory (Entra ID) und Azure-Dienste 162

Angriffsvektoren

Angriffe auf das Azure Active Directory und Azure-Dienste 168

Schutzmaßnahmen

Azure Active Directory und Azure-Dienste absichern 178

Zugriffsmanagement

Azure Active Directory und Zero Trust 185

Forensik und Logging

Angriffe auf Azure Active Directory entdecken und nachvollziehen 191

Threat Hunting

Angriffe auf Microsoft 365 aufspüren 197

Sonstiges

Editorial 3

Impressum 181

Inserentenverzeichnis 181

Angriffsszenarien

Durch Fehler bei der Konfiguration, mangelnde Härtung oder zu großzügige Rechtevergabe im Active Directory entstehen Einfallstore für Angriffe. Cyberkriminellen kann es dann gelingen, das gesamte AD zu übernehmen, um ihre kriminellen Ziele zu verfolgen. Nur wer weiß, wie die Kriminellen vorgehen und wie die verbreiteten Angriffe funktionieren, kann sich davor schützen.

ab Seite 41



Abwehrstrategien

Es gibt viele Ansätze, das AD vor Angreifern zu schützen. Die Bandbreite reicht von präventiven Maßnahmen mit Windows-Bordmitteln und Drittanbieterertools über Sicherheitsaudits bis hin zu grundlegenden Sicherheitsvorkehrungen, etwa nach IT-Grundschutz. Gelingt den Kriminellen trotzdem der Zugriff, muss der Angriff so schnell wie möglich entdeckt, forensisch aufbereitet und analysiert werden.

ab Seite 83



Azure AD / Entra ID

Wenn Unternehmen Microsoft 365 oder andere Dienste aus der Azure-Cloud einsetzen, nutzen sie den Cloud-Identitätsdienst Azure AD – vielleicht ohne sich dessen überhaupt bewusst zu sein. Wie beim On-Premises Active Directory können auch hier mangelnde Härtung und Fehlkonfigurationen dazu führen, dass Angreifer einzelne Identitäten, Ressourcen oder gar das komplette Azure AD kompromittieren – und schlimmstenfalls darüber Zugriff auf das lokale AD erlangen.

ab Seite 162



iX-Workshops rund um das (A)AD

iX veranstaltet in regelmäßigen Abständen Online-Workshops zu Active Directory und Entra ID (Azure AD). Sie richten sich an Administratorinnen und Administratoren, IT-Leiter, IT-Sicherheitsverantwortliche sowie an Security-Fachleute. In dem Workshop „Angriffsziel lokales Active Directory: effiziente Absicherung“ erfahren Sie an zwei Tagen, welche Techniken Angreifer einsetzen und welche Fehlkonfigurationen und Schwachstellen sie dabei ausnutzen. Sie lernen die wichtigs-

ten Härtungsmaßnahmen und Werkzeuge sowie Maßnahmen zum Erkennen und Abwehren von Angriffen kennen.

Der zweitägige Workshop „Angriffe auf und Absicherung von Entra ID (Azure Active Directory)“ zeigt, wie Angreifer Fehlkonfigurationen der Microsoft-Cloud sowie fehlende Härtungsmaßnahmen ausnutzen und man die AAD-Umgebung und Azure-Dienste effektiv absichert. Außerdem erfahren Sie, wie

Sie Angriffe auf Ihre Entra-ID-Umgebung durch Logging und Monitoring erkennen können.

Die beiden Sicherheitsschulungen halten je nach Termin Frank Ullly, der viele Artikel zu diesem Sonderheft beigetragen hat, oder sein Kollege Tim Mittermeier. Beide beschäftigen sich schwerpunktmäßig mit Pentesting und offensiver Sicherheit. Alle Termine finden Sie über ix.de/zqvy.