Noch immer Hackers Liebling

Als die erste Auflage dieses Sonderheftes im vergangenen Jahr kurz vor Druckschluss stand, wurden Netzwerke weltweit gerade mit einer besonders fiesen Datenlösch-Malware („Wiper“) geflutet, die über einen kompromittierten Active-Directory-Server auf sämtliche Rechner der betroffenen Unternehmen verteilt wurde. Das Active Directory hatte sich zum bevorzugten Einfallstor für Kriminelle und zu einer Verteilzentrale für Ransomware und Co. entwickelt.

Heute, rund eineinhalb Jahre später, sieht die Situation kein bisschen besser aus. Im Gegenteil: Ransomware- und andere Cyberangriffe sind mittlerweile Dauerthema auch in Nicht-Fachmedien und das Bundeskriminalamt bezeichnet in seinem aktuellen „Lagebild Cybercrime“* Ransomware als primäre Bedrohung für Unternehmen und öffentliche Einrichtungen. Im vergangenen Jahr, so der Bericht, wurde täglich mindestens ein deutsches Unternehmen Ziel eines Ransomware-Angriffs. Involviert ist dabei häufig das Active Directory, manche Forscher schätzen in bis zu 90 Prozent der von ihnen untersuchten Fälle.

Identitätsmissbrauch ist zum Mainstream geworden, sagt eine aktuelle Studie von Crowdstrike. Das Unternehmen beobachtet seit dem letzten Jahr einen Anstieg von Kerberoasting-Angriffen, die auf Passwörter von Service-Konten im Active Directory zielen, um 583 Prozent. Hinzu kommt, dass viele Unternehmen mit einem Mangel an Active-Directory-Expertise zu kämpfen haben, wie eine Umfrage ergab.

Die gute Nachricht ist: Wenn Sie dieses Heft in den Händen halten, haben Sie schon den ersten Schritt getan, sich das nötige Fachwissen anzueignen!

Mit dieser aktualisierten und erweiterten Neuauflage des iX kompakt zur AD-Sicherheit haben wir noch mal eine kräftige Schippe draufgelegt. Der erste Teil des über 200 Seiten starken Heftes versorgt Sie mit den Grundlagen zu AD und Azure AD, denn wenn man die Funktionsweise des Verzeichnisdienstes nicht kennt, ist eine ernsthafte Absicherung der Dienste nicht möglich. Über die in den weiteren Artikeln beschriebenen Angriffsflächen und Abwehrmaßnahmen hinaus hat sich seit dem letzten Heft einiges getan. So hat das BSI in Ausgabe 2023 seines IT-Grundschutzes das Sicherheitslevel im AD-Baustein noch einmal deutlich höher gehängt (ab Seite 136).

Zu dem Angriff PetitPotam, über den sich Kriminelle Goldene Zertifikate und damit Admin-Rechte im AD verschaffen können, ist ein weiterer hinzugekommen. Und auch das ist nur die Spitze eines Eisbergs. Microsoft hat zwar Maßnahmen gegen solchen Authentifizierungsmissbrauch ergriffen, die schließen aber nicht alle Lücken oder werden erst ab 2025 wirksam. Hier ist einiges an Handarbeit gefragt, was wir ab Seite 72 für Sie zusammengestellt haben.

Neu sind schließlich auch drei Praxisartikel, die einen Einstieg in das vielen noch als Tiering-Modell geläufige Sicherheitskonzept von Microsoft bieten (ab Seite 84). Das Enterprise Access Model, so der offizielle Name des deutlich komplexeren Nachfolgers, gilt vielen als Königsdisziplin der AD-Absicherung. Es basiert auf einer strikten Aufteilung administrativer Rechte und Zugriffe, letztere von speziell gehärteten Workstations aus. Das mag kleineren Unternehmen zunächst schwer umsetzbar erscheinen, aber das Modell lässt sich in verschiedenen Abstufungen realisieren, die auch schon in der weniger aufwendigen Variante einen deutlichen Sicherheitsgewinn bringen.

Microsoft hat eine Schwäche für Umbenennungen seiner Produkte und Konzepte, nicht nur des Tiering-Modells. Nun trifft es Azure Active Directory. Die neue Bezeichnung Entra ID wird bis Ende 2023 Schritt für Schritt in Produkten, Dokumentationen und Tech-Artikeln das alte Azure AD ersetzen. Wir haben uns für das vorliegende Heft dazu entschieden, die Umbenennung zwar zur allmählichen Umgewöhnung an der ein oder anderen Stelle zu erwähnen, im Großen und Ganzen aber die allen noch geläufige Bezeichnung Azure AD zu belassen.

Aber wie immer die Verzeichnis- und Identitätsdienste auch heißen: Geschützt werden müssen sie alle. Der Anfang mag schwer sein, aber jede Maßnahme hilft und ist ein Schritt in die richtige Richtung. Dieses Heft liefert Ihnen vielfältige Anregung und konkrete Anleitung. Legen Sie los!

UTE ROOS

* Alle zitierten Quellen und Studien sind über ix.de/zb8y zu finden.