Einloggen, statt Hacken: Missbrauch privilegierter Konten durch Cyberkriminelle

Für Cyberkriminelle ist der Missbrauch kompromittierter Anmeldedaten heute eine der beliebtesten Angriffstechniken. Statt sich in Systeme einzuhacken, die durch hochentwickelte Sicherheitstechnologien geschützt werden, nehmen Kriminelle mit ausgefeilten Social-Engineering-Attacken Mitarbeiter als das schwächste Glied in der Verteidigungskette ins Visier. Mit den erbeuteten Zugangsdaten loggen sie sich anschließend einfach ein. Dabei haben es Angreifer vor allem auf das Kapern von Konten mit umfangreichen Berechtigungen abgesehen. Diese liefern den goldenen Schlüssel zu Systemen und Netzwerkressourcen und bilden die perfekte Tarnung für Datenexfiltration oder Sabotage.
Einmal eingedrungen, bewegen sich Angreifer lateral, um das Netzwerk zu scannen, erhöhen gegebenenfalls ihre Privilegien und extrahieren sensibelste Daten wie Bankkonteninformationen, Geschäftsgeheimnisse oder geistiges Eigentum. Zuletzt verwischen sie ihre Spuren, sodass einem Unternehmen unter Umständen nicht einmal bewusst ist, dass sich die Angreifer monatelang im System aufgehalten haben. Darüber hinaus können Cyberkriminelle privilegierte Zugangsdaten nicht nur für eigene Attacken nutzen, sondern sie auch lukrativ durch Verkauf im Darknet zu Geld machen.

Laut dem Analystenhaus Forrester spielen kompromittierte privilegierte Zugangsdaten bei 80 Prozent aller Sicherheitsvorfälle eine Rolle (The Forrester Wave: Privileged Identity Management, Q4 2018). Um dieser wachsenden Bedrohung Herr zu werden, sollten Unternehmen deshalb ihre Sicherheitsbemühungen verstärkt auf die eigentliche Ursache des Problems konzentrieren: eine fehlende Kontrolle über ihre privilegierten Konten.

Fünf Best Practices gegen Missbrauch privilegierter Konten

Um Angreifern selbst im Fall eines Diebstahls privilegierter Log-in-Daten laterale Bewegung, Datendiebstahl und Sabotage unmöglich zu machen, benötigen Unternehmen einen mehrschichtigen Sicherheitsansatz aus Best Practices und Technologien. Die folgenden fünf grundlegende Maßnahmen helfen, den Missbrauch privilegierter Konten durch Cyberkriminelle zu minimieren:

1. Sicherheitstrainings für Mitarbeiter: Cyberkriminelle nutzen oft ausgefeilte Social-Engineering-Taktiken, um beispielsweise durch umfangreich recherchierte Spear-Phishing-Attacken an sensible Zugangsdaten zu gelangen. Regelmäßige und umfassende Sicherheitsschulungen, inklusive einer dezidierten Aufklärung der Benutzer über die Merkmale und Folgen von Phishing-Angriffen, sind deshalb ein wesentlicher erster Schritt, um das Risiko kompromittierter Anmeldedaten zu reduzieren.

2. Nutzerkonten-Erfassung und Passwort-Tresore: Dieser Schritt beginnt mit dem Erfassen und Registrieren aller Server, die ein Unternehmen in seiner Umgebung betreibt. Anschließend sollten alle von mehreren Usern verwendeten Konten, Alternate-Administrator-Konten sowie Dienst-Konten durch Passwort-Tresore geschützt sowie eine sichere Administrationsumgebung aufgebaut werden. Darüber hinaus sollten Auditing und die Überwachung von Sessions privilegierter Nutzer implementiert werden.

3. Identitätskonsolidierung und geringstmögliche Zugriffsberechtigungen: Zudem kann die Angriffsfläche weiter reduziert werden, indem Identitäten konsolidiert und lokale Konten so weit wie möglich eliminiert werden. Weiterhin sollten Kontrollen für die Berechtigungserweiterung implementiert werden sowie ein Just-in-Time-Privilegien-Zugriff: Dabei werden erforderliche Privilegien nur für einen begrenzten Zeitraum und/oder einen begrenzten Bereich vergeben.

4. Multi-Faktor-Authentifizierung (MFA) für privilegierte Benutzer: Eine der einfachsten Methoden ist darüber hinaus die Implementierung einer Multi-Faktor-Authentifizierung für alle privilegierten Benutzer. MFA ist eine der besten Möglichkeiten, um zu verhindern, dass unbefugte User auf sensible Daten zugreifen und sich lateral im Netzwerk bewegen können. Daher sollte eine MFA-Implementierung für alle Unternehmen Standard sein, insbesondere wenn es um den Schutz von Privilegien geht.

5. Härtung der Umgebung durch Air-Gaping und mit Hilfe von Machine Learning: Der letzte Schritt besteht darin, die Umgebung durch Air-Gaping, also einer logischen Isolation der Administrationskonten voneinander, zu härten, wie es Microsoft‘s Konzept der Enhanced Security Administration Environment (ESAE) vorschlägt. Um Angreifern keinerlei Umgehungsmöglichkeiten zu bieten, sollten zudem die Überwachung von Befehlen und die Verhaltensanalyse privilegierter Nutzer auf Basis von Machine Learning (User Behavior Analytics, UBA) eingesetzt werden. Diese Lösungen schlagen bei anormalen und verdächtigen Aktivitäten umgehend Alarm. Für die sensibelsten Umgebungen kann darüber hinaus noch eine Multi-Faktor-Authentifizierung der Sicherheitsstufe 3 hinzugefügt werden.

Sicherheitstechnologien wie Privileged Access Management-Lösungen (PAM) mit dezidiertem Zero Trust-Ansatz ermöglichen es hier, Nutzern nur den Zugriff mit den unbedingt erforderlichen Berechtigungen („Least Privilege") zu gewähren. Dies geschieht, basierend auf der Überprüfung, wer den Zugriff anfordert, dem Kontext der Anforderung und dem Risiko der Zugriffsumgebung. Da sich traditionelle Netzwerk-Perimeter zunehmend auflösen, bietet eine PAM-Lösung mit Least-Privilege- und Zero-Trust-Ansatz sowohl kleinen und mittleren Unternehmen als auch großen Organisationen mit komplexen, heterogenen und agilen Infrastrukturen mit DevOps, Cloud-Instanzen und Containers umfassenden Schutz ihrer privilegierter Konten.

Für Cyberkriminelle ist der Diebstahl privilegierter Anmeldedaten und deren Missbrauch für den Zugriff auf ein Netzwerk in der Regel einfacher, effizienter und weniger riskant als das Ausnutzen einer bestehenden Schwachstelle – selbst eines Zero-Day-Exploits. Deshalb ist für Unternehmen ein mehrschichtiger Sicherheitsansatz, bestehend aus Sicherheitstrainings und der umfassenden Stärkung ihrer Authentifizierungssysteme, eine wichtige Voraussetzung, um Cyberangriffe durch Privileged Access Abuse abzuwehren.