Sicher aus der Ferne: Privileged Access für Remote-Administratoren - Sechs Best Practices für Fernzugriff auf kritische Infrastrukturen

Viele Unternehmen verfügen über Richtlinien und Lösungen für die Telearbeit, doch diese sind meist auf Mitarbeiter zugeschnitten, die vollständig remote agieren oder normalerweise im Büro arbeiten, aber Flexibilität für ungewöhnliche Situationen benötigen. Die derzeitige Lage, mit der die meisten Unternehmen konfrontiert sind, kann die Fähigkeiten ihrer Remote-Arbeitsplätze auf die Probe stellen. Dies gilt insbesondere hinsichtlich Security-Kontrollen, Cyber-Hygiene und der Reduzierung von Sicherheitsrisiken, die eine Remote-Belegschaft mit sich bringt.

Handelt es sich um IT-Administrationsteams, ausgelagerte IT und Drittanbieter, die eventuell privilegierten Zugriff auf Systeme und Infrastruktur haben, benötigen diese einen sicheren, granularen Zugang zu kritischen Infrastrukturressourcen, unabhängig vom Standort und ohne die Security-Problematik eines Virtual Private Networks (VPN). Im Idealfall sollte sich der privilegierte Zugriff auf diese Systeme nicht unterscheiden, egal ob sich die Benutzer in einem lokalen Rechenzentrum befinden oder, ob sie von außerhalb auf diese Systeme zugreifen.

VPN als Sicherheitsrisiko bei Zugriff auf kritische Ressourcen

Letztes Jahr erlitt Citrix durch einen Password-Spraying-Angriff, der auch den VPN-Zugang zu nutzen versuchte, einen Sicherheitsverstoß. Beim Password-Spraying verwenden Angreifer mittels Brute Force ein häufig genutztes Passwort gegen eine große Anzahl von Benutzerkonten. Diese Technik ermöglicht es Cyberkriminellen, unentdeckt zu bleiben, indem schnelle oder häufige Kontosperren vermieden werden. Jüngst wurden auch US-Energieunternehmen zur Zielscheibe von Angreifern, die Password-Spraying und VPN-Hacking nutzten.

Im Gegensatz zu einem VPN, das Benutzern in der Regel Einblick in das gesamte Netzwerk gewährt, sollten Unternehmen deshalb den Zugriff auf Ressourcen nur auf der Basis der jeweils benötigten Berechtigungen gewähren. Dadurch erhalten privilegierte interne IT-Administratoren lediglich Zugriff auf so viel Infrastruktur wie nötig, während der Zugang eines ausgelagerten Teams auf die Server und Netzwerk-Hardware beschränkt wird, die für ihre Aufgabe erforderlich sind. Privilegierte Benutzer sollten sich entweder über Active Directory, LDAP oder einem anderen maßgeblichen Identitätsspeicher authentifizieren, oder Geschäftspartnern und Drittanbietern sollte ein vereinter granularer, privilegierter Zugriff auf Ressourcen gewährt werden.

Zum Schutz vor Cyber-Angriffen ist deshalb eine Kombination aus rollenbasierten Zugriffskontrollen mit dem jeweiligen Risiko-Level, Benutzerkontext und einer Multi-Faktor-Authentifizierung empfehlenswert. Dies ermöglicht intelligente, automatisierte Echtzeit-Entscheidungen für die Gewährung von Zugangsberechtigungen für Benutzer beim Remote-Zugriff auf Server, dem Auschecken von Passwörtern oder bei der Verwendung eines gemeinsamen Kontos zur Anmeldung bei Remote-Systemen.

Sicherer Privileged Access für Vor-Ort- und Remote-Administration

Im Folgenden sechs Möglichkeiten, wie Unternehmen Konsistenz in ihrem Privileged Access Management-Ansatz (PAM) schaffen können, um den Fernzugriff auf Rechenzentrums- und Cloud-basierte Infrastrukturen durch einen Cloud-basierten Service oder die Bereitstellung on-Premises zu schützen:

1. Abgesicherter, kontextbezogener Zugriff für IT-Administratoren auf einen kontrollierten Satz von Servern, Netzwerkgeräten und Infrastructure-as-a-Service (IaaS).

2. Ermöglichung einer ausgelagerten IT, ohne dass Administratoren in das Active Directory aufgenommen werden müssen.

3. Zugriffskontrolle zu ausgewählten Rechenzentrums- und Cloud-basierten Ressourcen, ohne das erhöhte Risiko eines vollständigen VPN-Zugriffs einzugehen.

4. Absicherung des gesamten administrativen Zugriffs mit risikobewusster Multi-Faktor-Authentifizierung (MFA).

5. Ein einziger sicherer Zugriffspunkt für Administratoren zur Verwaltung der Infrastruktur mit gemeinsam genutzten Konten oder ihrem eigenen Active Directory-Konto.

6. Sicherer Fernzugriff auf Rechenzentrums- und Cloud-basierte Infrastrukturen für interne Benutzer, Drittanbieter und

ausgelagerte IT über einen Cloud-Service oder die Bereitstellung vor Ort.

Sich auf VPNs zu verlassen, anstatt konsistente Sicherheitsprozesse und -Richtlinien einzuführen, birgt ein erhöhtes Risiko für kritische IT-Ressourcen. Unternehmen können ihre Sicherheitsposition erheblich stärken, indem sie intelligente, automatisierte Echtzeit-Entscheidungen für die Gewährung privilegierter Zugriffsberechtigungen auf Systeme und Infrastrukturen implementieren. Damit sind sie auch für eine große Anzahl von Mitarbeitern an Remote-Standorten gut vorbereitet, einschließlich privilegierter Administratoren.