

3-Schritte-Guide: Privilegierten Zugriff problemlos verwalten und schützen

Die effektive Verwaltung von Berechtigungen und Zugangsdaten ist für die Sicherheit Ihres Unternehmens unerlässlich. Da **74 % der Datenpannen** auf den Missbrauch privilegierter Konten zurückzuführen sind, ist das ein Bereich, mit dem sich Unternehmen befassen müssen. Cyberangreifer können Zugangsdaten auf verschiedene Weise missbrauchen. Häufig werden Social Engineering und Phishing eingesetzt sowie eine mangelhafte Passworthygiene oder das Wiederverwenden von Passwörtern ausgenutzt. Oder aber die Angreifer bedienen sich sogenannter Initial Access Broker, die Zugangsdaten im Dark Web verkaufen.

Um dem entgegenzuwirken, ist es wichtig, die Art und Weise, wie Sie Ihre privilegierten Konten verwalten, zu optimieren. Die folgenden drei Schritte machen die Verwaltung und Absicherung privilegierter Konten einfacher und verringern die Wahrscheinlichkeit interner und externer Angriffe:

1. Vereinfachen Sie Ihr Compliance-Reporting



2. Nutzen Sie Zero Trust Network Access



3. Bieten Sie Dienstleistern sicheren Zugriff auf Ihre Unternehmensumgebung





1. Vereinfachen Sie Ihr Compliance-Reporting

Um Kunden zu zeigen, dass die Zusammenarbeit mit Ihrem Unternehmen im Hinblick auf Netzwerk- und Datensicherheit nachweislich sicher ist, sind hohe Compliance-Standards von großer Bedeutung. Zertifizierungen von Organisationen wie der [Internationalen Organisation für Normung \(ISO\)](#) und dem National Institute of Standards and Technology (NIST) sind eine gute Möglichkeit, Ihre Kunden davon zu überzeugen, dass sie Ihnen ihre Daten anvertrauen können. Um diese Zertifizierungen zu bekommen bzw. zu behalten, führt die ISO einmal jährlich ein Audit durch, um zu überprüfen, ob Sie ihre Standards einhalten.

CloudGen Access listet automatisch und übersichtlich auf, wer, wozu und wann privilegierte Konten genutzt hat und protokolliert Identität, Gerät und Standort aller Benutzer, die versuchen, erfolgreich oder nicht, auf Ihr Netzwerk zuzugreifen. Diese Aufzeichnungen können den Prüfern dann ohne manuelle Nachverfolgung oder Eingabe von Daten präsentiert werden. Die Funktion wird im Hintergrund ausgeführt, d. h. Sie müssen weder Zeit, Mühe noch Kosten aufwenden, um diese Aufzeichnungen zu erhalten und Ihre Daten vor einem Audit auch nicht auf Korrektheit und Aktualität prüfen – das ist bereits geschehen. Sie können diese Protokolle auch zur Erstellung übersichtlicher Berichte über den Systemzugriff im gesamten Unternehmen nutzen, falls andere Stellen diese Information benötigen.



2. Nutzen Sie Zero Trust Network Access

Zero Trust Network Access (ZTNA) hat sich in den letzten Jahren zu einer Art Modewort entwickelt, dem von Personen und Unternehmen allerlei Bedeutung aufgeladen wurde. Einfach gesagt, ist ZTNA eine Philosophie zur Netzwerksicherheit, die auf dem Prinzip basiert, bis zu einer erfolgreichen Verifizierung nichts und niemandem zu vertrauen. Angesichts des Anstiegs von Remote- und Hybrid-Arbeit seit dem Ausbruch der COVID-19-Pandemie und der verstärkten Nutzung der Cloud war es noch nie so wichtig, Benutzer und Geräte, die versuchen, von außerhalb auf Ihr Netzwerk zuzugreifen, zu verifizieren und zu verwalten.

Mit dieser Lösung werden veraltete VPNs oder andere komplizierte Methoden des Netzwerkzugriffs obsolet. ZTNA ermöglicht die schnelle und einfache Implementierung einer beispiellosen Zugriffskontrolle für alle Benutzer und Geräte. So können Mitarbeiter und Partner auf alle Web-Applikationen und Cloud-Workloads zugreifen, für die sie eine Berechtigung haben, ohne die Angriffsfläche zu vergrößern. Anstatt den Zugriff mit Barrieren wie der mehrfachen Eingabe von Anmeldedaten zu erschweren, stattdessen das Netzwerk mit Schutzebenen aus, die den Zugriff beschleunigen. Indem jeder Netzwerkbenutzer nur Berechtigungen für die Anwendungen und Workloads erhält, die er für seine Aufgaben benötigt, können Sie dafür sorgen, dass jeder Benutzer genau die Zugriffsrechte besitzt, die er braucht – nicht mehr und nicht weniger.

3



3. Bieten Sie Dienstleistern sicheren Zugriff auf Ihre Unternehmensumgebung

Der Zugriff Dritter auf die Systeme und Anwendungen Ihres Unternehmens ist oft unvermeidbar, bietet aber auch Vorteile. So können Sie gezielt geeignete Arbeitspartner auswählen, ohne durch den Standort oder interne Kompetenzen eingeschränkt zu sein. Dies macht jedoch eine weitere Sicherheitsebene notwendig, um Risiken, die durch die Zugriffsvergabe für Ihre Anwendungen und Systeme entstehen, zu reduzieren. Andernfalls könnte es sein, dass Bedrohungen ihre Netzwerkgrenzen überwinden.

CloudGen Access ermöglicht die Vergabe von rollenbasiertem, sicheren Zugriff auf Anwendungen und Daten und sorgt dafür, dass Dritte nur auf das zugreifen können, was sie für ihre Aufgaben benötigen. Wir sprechen hier also eher von Ressourcenzugriff als von Netzwerkzugriff. Dritte benötigen keinen Zugriff auf Ihr gesamtes Netzwerk. Deshalb ist es viel effizienter und sicherer, ihnen nur Zugang zu den Ressourcen und Anwendungen zu gewähren, die sie brauchen.

Um sicherzustellen, dass nur verifizierte Benutzer auf das gesamte Netzwerk zugreifen können, generiert und speichert das System ein Gerätezertifikat auf einem Hardware-Keystore, das für das Gerät als ID dient. Kommt der richtige Login auf einem anderen Gerät zum Einsatz, das möglicherweise weniger sicher ist, wird der Zugriff automatisch verweigert. Zugriff wird nur kontextbezogen und bedingt gewährt, was bedeutet, dass Sie die optimale Kontrolle darüber haben, wer von welchem Gerät aus auf Ihre Systeme zugreift.

Die Zeit ist reif für den Einsatz von ZTNA

Da die Nutzung privilegierter Konten in den letzten Jahren so viele erfolgreiche Datenpannen verursacht hat, müssen Unternehmen Maßnahmen zur sicheren Verwaltung der Berechtigungen und des Netzwerkzugriffs ergreifen, bevor es zu spät ist.

Testen Sie Barracuda CloudGen Access kostenlos 14 Tage lang und überzeugen Sie sich selbst davon, wie leicht es ist, Ihre Compliance zu vereinfachen, Zero Trust Network Access zu implementieren und den Zugriff Dritter auf Ihre Systeme zu sichern. Wenn Sie Fragen haben, können Sie uns auch gerne kontaktieren

de.barracuda.com/company/contact.



Über Barracuda

Barracuda ist bestrebt, die Welt zu einem sichereren Ort zu machen und überzeugt davon, dass jedes Unternehmen Zugang zu Cloud-fähigen Sicherheitslösungen auf höchstem Niveau verdient, die einfach zu erwerben, zu implementieren und zu nutzen sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die im Zuge der Customer Journey wachsen. Mehr als 200.000 Unternehmen weltweit vertrauen auf Barracuda und darauf, dass wir sie auch vor Risiken schützen, die ihnen möglicherweise gar nicht bewusst sind. Daher können sich diese Unternehmen ganz auf ihr Wachstum konzentrieren. Weitere Informationen finden Sie auf de.barracuda.com.

