CLOUDFLARE®

Der Zero Trust-Leitfaden: So sichern Sie den Anwendungszugriff durch Auftragnehmer

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

I. Kurzfassung

Mitarbeitern außerhalb Ihrer Organisation Zugriff auf Anwendungen zu gewähren — unabhängig davon, ob es sich dabei um Leiharbeiter, Agenturen oder Partnerorganisationen handelt — kann ein Sicherheitsrisiko und eine erhebliche logistische Herausforderung darstellen. Viele moderne Anwendugen sind nicht mit traditionellen Plattformen für Identitäts- und Zugriffsverwaltung (Identity and Access Management – IAM) kompatibel, so dass man auf provisorische Systeme angewiesen ist, die schwer zu verwalten sind.

Zero Trust Network Access ist eine Möglichkeit, diese Herausforderungen zu überwinden. Möglich wird dies durch die Anwendung des Prinzips der geringsten Berechtigung auf geschäftskritische Anwendungen. Dies umfasst den Einsatz von Mikroperimetern um jede Anwendung herum, das Verbergen von Anwendungen hinter verschlüsselten Verbindungstunneln und die Protokollierung jeder Anfrage. Dadurch können Unternehmen die Prozesse rund um IAM vereinfachen, wertvolle Entwicklungszeit freisetzen und die Möglichkeiten für Datenverluste erheblich reduzieren.

TEIL 1

Das Prinzip der geringsten Berechtigung: Ziele und Herausforderungen

Zugriffsverwaltung ist eines der grundlegendsten Ziele eines jeden Enterprise Security-Programms. Um proprietäre Daten, kritische Systeme und die Produktqualität zu schützen, arbeiten die Sicherheitsverantwortlichen an der Umsetzung des Prinzips der geringsten Berechtigung (Principle of Least Privilege – POLP). Dieses verlangt, dass die Benutzer nur auf jene Ressourcen zugreifen können, die sie zur Ausübung ihrer Arbeit benötigen, und dass ihr Zugriff auf die Dauer beschränkt wird, für die er benötigt wird.

Dieses Ziel ist besonders wichtig im Fall von Auftragnehmern, Lieferanten, Partnern und anderen vertrauenswürdigen Dritten. Diese Benutzer werden oft zur Durchführung bestimmter Aufgaben oder Projekte an Bord geholt, so dass ihr Zugriff mit besonderer Sorgfalt verwaltet werden sollte.

Grundsätzlich helfen IAM-Plattformen Organisationen in diesen Fällen bei der Umsetzung des POLP durch:

- Definieren von Listen bekannter Benutzer (Verzeichnis)
- Erleichterung ihrer Zugriffe auf der Grundlage definierter Kriterien (Authentifizierung)
- Beschränkung ihrer Berechtigungen auf das, worauf sie zugreifen können sollten (Autorisierung)
- Periodische Anpassung ihres Zugriffs auf bestimmte Ressourcen (Lebenszyklus)

Leider sieht IAM in der Praxis oft anders aus. Im Folgenden erörtern wir einige der Herausforderungen, die bei der Erreichung dieser Ziele zu bewältigen sind.

Herausforderung Nr. 1: Integration verschiedener Anwendungen mit einem IAM-System

Die meisten großen Organisationen betreiben eine komplexe, heterogene Anwendungs- und Infrastrukturumgebung. Bestimmte Software-as-a-Service (SaaS) und On-Premises-Anwendungen eignen sich gut für die standardbasierten Authentifizierungsmethoden von IAM-Plattformen. Viele Anwendungen können allerdings nur sehr schwer oder gar nicht in diese Plattformen integriert werden. Gartner schätzt, dass derzeit nur 30 Prozent der Single-Sign-On-Transaktionen moderne Identitätsprotokolle wie SAML, OAUTH2 und OIDC 1 verwenden. Die anderen 70 Prozent der nicht standardbasierten Transaktionen betreffen Legacy-Protokolle oder benutzerdefinierte Frameworks, die sich nicht einfach in traditionelle IAM-Plattformen integrieren lassen und deren Sicherung zusätzlichen Zeit- und Entwicklungsaufwand erfordert. Übliche Anwendungen, die in die letztere Kategorie fallen, umfassen:

- **Intern gehostete Anwendungen** (einschließlich intern entwickelter privater Anwendungen und privat gehosteter Cloud-Anwendungen)
  - Atlassian-Apps
  - Drupal
  - Grafana
  - JIRA
  - Splunk
  - DataDog
  - Gitlab
  - Bitbucket
- **Infrastructure**
  - Amazon Web Services (AWS)
  - Google Cloud Platform (GCP)
  - Microsoft Azure

Um diese Probleme zu überwinden, greifen Organisationen in der Regel auf folgende Ansätze zurück:

Methode	Herausforderungen und Risiken
Zuweisen separater Benutzernamen und Passwörter für Anwendungen, die nicht mit der zentralen IAM-Plattform kompatibel sind.	Die Organisation verfügt auch über weitere Benutzeridentitäten, für die Verwaltung, Onboarding und Offboarding erforderlich sind.
Bereitstellung von Anwendungen über ein virtuelles privates Netzwerk (VPN).	Die Organisation muss also quasi eine Lücke in ihre Netzwerk-Firewall bohren, um den Benutzern den Zugriff mit einem VPN oder einem Remote-VPN-Agent zu ermöglichen.
Erstellung und Wartung benutzerdefinierter Software auf privaten Anwendungsservern, um Single Sign-On (SSO) zu ermöglichen.	Die Organisation muss den Entwicklern kontinuierlich erhebliche Anstrengungen abverlangen.

Herausforderung Nr. 2: Drittbenutzer bringen einzigartige Komplexität

Externe Benutzer bringen noch weitere Herausforderungen mit sich. Da diese Benutzer oft remote oder befristet arbeiten, greifen Sicherheitsbeauftragte in der Regel auf die folgenden Ansätze zurück: Beide sind schwierig zu implementieren und potenziell unsicher:

Methode	Herausforderungen und Risiken
Zuweisen separater Benutzernamen und Passwörter für Anwendungen, die nicht mit der zentralen IAM-Plattform kompatibel sind.	• Die Organisation verfügt auch über weitere Benutzeridentitäten, für die Verwaltung, Onboarding und Offboarding erforderlich sind.
Bereitstellung von Anwendungen über ein virtuelles privates Netzwerk (VPN).	• Die Organisation muss also quasi eine Lücke in ihre Netzwerk-Firewall bohren, um den Benutzern den Zugriff mit einem VPN oder einem Remote-VPN-Agent zu ermöglichen.
Erstellung und Wartung benutzerdefinierter Software auf privaten Anwendungsservern, um Single Sign-On (SSO) zu ermöglichen.	• Die Organisation muss den Entwicklern kontinuierlich erhebliche Anstrengungen abverlangen.

Herausforderung Nr. 2: Drittbenutzer bringen einzigartige Komplexität

Externe Benutzer bringen noch weitere Herausforderungen mit sich. Da diese Benutzer oft remote oder befristet arbeiten, greifen Sicherheitsbeauftragte in der Regel auf die folgenden Ansätze zurück: Beide sind schwierig zu implementieren und potenziell unsicher:

Methode	Herausforderungen und Risiken
Zuweisen eines VPN an Drittbenutzer	• Zeitaufwändig und teuer in der Zuweisung für neue Benutzer; insbesondere, wenn es die Ausgabe physischer Maschinen an Auftragnehmer erfordert • Risiko lateraler Bewegung, sobald ein Benutzer verbunden ist • Risiko des Datenverlusts, da Benutzer personenbezogene Daten (Personally Identifiable Information – PII) auf persönlichen Computern speichern können
Erstellen von Firmen-Benutzeridentitäten für Drittbenutzer	• Zeitaufwändiger manueller Prozess, um Benutzerkonten den richtigen Personen zuzuweisen • Die Organisation wird verantwortlich für die Verwaltung des Onboarding, Offboarding und der Berechtigungen des Kontos und übernimmt die Kosten für zusätzliche Benutzer in Identitätsmanagement-Plattformen • Zusätzliche Kommunikation zwischen Abteilungen wie HR und IT erforderlich
Verbinden der IAM-Plattform mit einer bestehenden Plattform, die vom Drittanbieter verwaltet wird	• Zeitaufwändiger Prozess zur Integration von Plattformen und zur Erstellung einmaliger Genehmigungsregeln. • Mögliche Inkompatibilität zwischen Plattformen • Selten durchführbar für einzelne Dritte

TEIL 2

Die Vorteile von Zero Trust Network Access

Zero Trust Network Access (ZTNA) ist ein Framework zur Bewältigung dieser Herausforderungen. Es basiert auf dem Grundsatz, dass ein Unternehmen zu keinem Zeitpunkt irgendeinem Benutzer oder Gerät trauen sollte, unabhängig davon, ob sich diese innerhalb oder außerhalb des eigenen Perimeters befinden. Es mildert Sicherheitsbedenken im Zusammenhang mit dem Zugriff Dritter, indem es keinen allgemeinen, sondern einen spezifischen Zugriff zu Ihren internen Ressourcen vorsieht.

Zero Trust Network Access erreicht dies durch:

- Entfernen interner Anwendungen aus dem virtuellen privaten Netzwerk und Erstellen einer logischen Zugriffsbegrenzung um jede von ihnen
- Verbergen von Anwendungen hinter verschlüsselten Verbindungstunneln
- Protokollierung jeder Anfrage, die an interne Ressourcen gestellt wird (sowohl Anfragen zur Authentifizierung als auch Anfragen innerhalb der Anwendung selbst), um die Sichtbarkeit zu erhöhen

Diese Schritte ermöglichen es Unternehmen effektiv, die granularen Zugriffskontrollen, die sie in ihrem bestehenden Identitätsanbieter implementiert haben, auf intern verwaltete Anwendungen und Infrastruktur anzuwenden. Außerdem können Organisationen Drittbenutzern auf Anwendungsebene Zugriff auf ihre internen Ressourcen gewähren und Benutzern aus mehreren Organisationen Zugriff auf intern gehostete Ressourcen mit ihrer eigenen Corporate Identity gewähren.

Hier ist ein Beispiel dafür, wie dieses Framework angewandt werden kann.

Zero Trust Network Access: Anwendungsbeispiel

Die Entwicklung neuer Apps und Services ist eine gemeinschaftliche Anstrengung, und viele Organisationen entwickeln neue Produkte mit kombinierten Teams von Auftragnehmern und Vollzeitmitarbeitern. Der Schutz der Entwicklungsanwendungen und -umgebungen einer Organisation kann in folgenden Fällen eine Herausforderung darstellen:

- Die Organisation verfügt über unternehmenskritische Infrastruktur (z.B. Virtual Private Clouds) und Anwendungen (BitBucket, Git-Workflows usw.), die SSH-Zugang benötigen
- Die Produktteams sind teilweise auf unterschiedliche Standorte verteilt, auch in anderen Ländern
- Remote-Entwickler haben über VPN Zugang zu Entwicklungsumgebungen und Anwendungen, was die Verbindungsgeschwindigkeit verlangsamen und zusätzliche Risiken mit sich bringen kann

Zero Trust Network Access kann diesen Herausforderungen begegnen durch:

1. Sicherung des Remote-Zugriffs auf geschäftskritische Infrastruktur
2. Sperren von Entwicklungs- und Bereitstellungsstandorten, bevor sie die Produktion erreichen
3. Schützen anderer interner Anwendungen, auf die Entwickler angewiesen sind (z.B. GitHub, Jira)

TEIL 3

Implementierung von Zero Trust Network Access in Ihrer Organisation

Zero Trust Network Access kann Ihre Prozesse sichern und beschleunigen, um vertrauenswürdigen Drittbenutzern Zugang zu internen Anwendungen und Ressourcen zu ermöglichen. Nach der Implementierung müssen Dritte kein VPN verwenden, um auf Ihre Anwendungen zuzugreifen; sie können sich stattdessen mit einem von Ihrer Organisation definierten Authentifizierungsverfahren anmelden.

Änderungen an Ihrer Anmeldungserfahrung haben einen großen Einfluss auf die Benutzer. Um es richtig zu machen, bedarf es teamübergreifender Kommunikation und Planung. Erfolgreiche Programme beginnen oft mit einer kleinen Pilotgruppe von Benutzern und einer Zielanwendung. Wir empfehlen, einen Index der intern verwalteten Anwendungen zu erstellen und festzulegen, auf welche davon Auftragnehmer und andere externe Parteien zugreifen müssen.

Verwenden Sie ab hier den Index, um eine Anwendung zu identifizieren, die mit einer Testgruppe als Pilot für ZTNA getestet werden soll. Vorrang sollten Anwendungen haben, die die folgenden Kriterien erfüllen:

- Webanwendungen
- Anwendungen, die HTTPS verwenden
- Nicht geschützt bei bestehenden SSO-Anbietern
- Wird von 5-10 % der gesamten Firmenbelegschaft verwendet

Hier ist ein Beispiel für einen solchen Index:

Anwendung/ Ressource	Wer darauf zugreift	Heutiger Onboarding-Prozess	Anzahl der betroffenen Benutzer	Bereit für ZTNA-Pilot (1-5)
Grafana	Intern – Rechnungsabteilung Extern – Berater	Azure-AD + VPN	45	4
Drupal	Intern – Marketing, Support Extern: Offshore Entwicklung	Azure-AD + VPN	1000	3
Jira	Intern – alle Abteilungen Extern – viele Auftragnehmerteams	Azure-AD + VPN	10.000	1

Nachdem Sie die richtige Pilotanwendung und Auftragnehmer-Nutzergruppe identifiziert und die Anwendung auf die richtige Größe getestet haben, sollten Sie sich überlegen, wie Sie den Zugang von Auftragnehmern zu Ihren Systemen identifizieren und überprüfen wollen. Wenn Sie für ZTNA einen starken Lieferantenpartner gewählt haben, haben Sie mehrere Möglichkeiten, wie Sie den Partnern den Zugang ermöglichen können:

Option 1: Erlauben Sie Auftragnehmern, sich bei ihrem SSO-Provider anzumelden

Wenn die externe Organisation, mit der Sie zusammenarbeiten, SSO verwendet, um Zugriff auf ihre Anwendungen zu gewähren, können Sie den Auftragnehmern gestatten, sich bei Ihrer Anwendung mit ihrer eigenen Corporate Identity anzumelden.

Dieser Ansatz kann gut geeignet sein, wenn:

- Sie Zeit damit verbringen können, im Vorfeld einen Verbund zwischen Ihrem SSO und dem SSO der Partnerorganisation aufzubauen
- Sie die Vorteile sicherer Zugriffsrichtlinien wie Multi-Faktor-Authentifizierung (MFA) nutzen möchten, die im SSO der Auftragnehmerorganisation implementiert wurden
- Sie den Lebenszyklus der Identität des Auftragnehmers nicht verwalten möchten, wenn er Ihre Organisation verlässt: Die Identität ist nur so lange gültig, wie der Benutzer im Verzeichnis der Auftragnehmerorganisation eingetragen ist

Anwendungsbeispiel:

1. Josef von Firma A meldet sich mit seinem Benutzernamen und Passwort von Firma A über SSO bei seiner CRM-Plattform an.
2. Wenn er sich bei Ihrer Anwendung anmeldet, wird er auf die Anmeldeseite von Firma A weitergeleitet, um sich mit seinen Firmendaten anzumelden.
3. Wenn er durch das SSO verifiziert wurde und in Ihrer ZTNA-Plattform Zugriff auf die Anwendung erhalten hat, kann Josef auf die Anwendung zugreifen.

Option 2: Verwenden Sie E-Mail-Einmal-PINs, um Partner-Anmeldung bereitzustellen

Wenn Sie Auftragnehmern Zugang zu einer bestimmten Anwendung geben müssen, aber keinen Verbund mit dem Identitätsprovider (IDP) einer anderen Organisation aufbauen möchten, sind E-Mail-Einmal-PINs (OTP) eine einfache Methode zur Authentifizierung. Bei diesem Ansatz gibt Ihre Organisation einer Gruppe von Auftragnehmern mit einer einfachen Liste von E-Mail-Adressen Zugriff auf die Anwendung und stellt den E-Mail-Adressen dieser Benutzer jedes Mal, wenn diese sich bei Ihrem Service anmelden müssen, eindeutige Anmeldecodes zur Verfügung.

Dieser Ansatz kann gut geeignet sein, wenn:

- Sie dem Auftragnehmer kein IDP-Unternehmenskonto ausstellen möchten
- Sie keinen Verbund mit dem SSO des Auftragnehmers aufbauen möchten
- Sie den E-Mail-Zugriff als eine geeignete Vertrauensebene für den Anwendungszugriff betrachten
- Sie mit Auftragnehmern aus mehreren Organisationen zusammenarbeiten

Beispiel für einen Ablauf:

1. Karin von Unternehmen B arbeitet mit Ihrem Marketingteam an einer neuen Landing Page. Die Staging-Website wird in Ihrem CMS gehostet.
2. Wenn Karin auf das CMS zugreift, um an dem Entwurf zu arbeiten, wird sie gebeten, ihre E-Mail-Adresse einzugeben.
3. Beim Abrufen Ihrer E-Mails erhält sie einen Code, den sie kopieren und in den Anmeldebildschirm für den Zugang einfügen kann.

Option 3: Verwendung einer vereinbarten Social Identity

In einigen Szenarien möchten Sie es Auftragnehmern ermöglichen, Social Identity-Provider wie GitHub oder LinkedIn für den Zugriff auf Ihre Anwendung zu nutzen.

Dieser Ansatz kann gut geeignet sein, wenn:

- Sie mit Benutzern aus kleinen Organisationen zusammenarbeiten, die keine Corporate Identity Management-Systeme verwenden
- Sie ein gemeinsames Framework (GitHub, LinkedIn) zur Authentifizierung von Auftragnehmern aus mehreren verschiedenen Organisationen benötigen

Beispiel für einen Ablauf:

Robert ist ein Anbieter, der mit Ihrem Entwicklungsteam an der Qualitätssicherung einer neuen mobilen Anwendung arbeitet. Wenn er versucht, sich bei Ihrer Webanwendung anzumelden, wird er zu seinem LinkedIn-Anmeldebildschirm umgeleitet. Wenn er sich erfolgreich bei LinkedIn anmeldet, erhält er Zugriff zu Ihrer Anwendung.

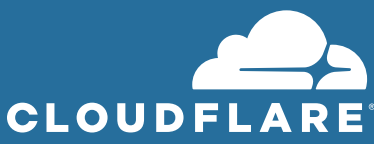
Wie Cloudflare bei der Implementierung von Zero Trust Network Access helfen kann

Cloudflare für Teams ist das Angebot von Cloudflare, das Unternehmen bei der Sicherung ihrer Geräte, Netzwerke und internen Anwendungen unterstützt. Es schützt die Verbindungen Ihres Teams im offenen Internet, bietet blitzschnellen Zugriff und ermöglicht es Ihnen, den Benutzerzugriff auf Anwendungen zu kontrollieren und die Zero Trust-Architektur zu nutzen.

Um nähere Informationen zu erhalten und mit einem Mitglied unseres Teams zu sprechen, besuchen Sie teams.cloudflare.com.

Endnoten

1. „Magic Quadrant for Access Management 2019“, Gartner, https://www.gartner.com/en/documents/3956209/magic-quadrant-for-access-management, abgerufen am 24. Februar 2020



+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

REV: 200318