wallix

WALLIX Guide

So schützen Sie Ihr Unternehmen vor identitätsbasierten Angriffen



WALLIX Guide

So schützen Sie Ihr Unternehmen vor identitätsbasierten Angriffen

1. Einleitung

Identity Security bezeichnet den Schutz digitaler Identitäten – also der Konten, Zugangsdaten und Berechtigungen, über die Menschen, Maschinen und Dienste auf die Systeme eines Unternehmens zugreifen. Ihre Bedeutung nimmt stetig zu, denn Identitäten sind heute eine der zentralen Angriffsflächen. Die meisten Sicherheitsverletzungen beginnen nicht mehr damit, dass Angreifer eine klassische Netzwerkgrenze überwinden. Häufig stehen gestohlene Zugangsdaten, durch Phishing kompromittierte Sitzungen oder der unbemerkte Missbrauch überprivilegierter Konten am Anfang eines Angriffs.

Der Diebstahl von Zugangsdaten und Phishing gehören weiterhin zu den häufigsten Einfallstoren. Dabei gelingt es Angreifern zunehmend, einfache MFA-Verfahren mithilfe sogenannter Adversary-in-the-Middle-Techniken zu umgehen. Haben sie sich erst einmal Zugang verschafft, nutzen sie übermäßige oder nicht mehr benötigte Berechtigungen, um sich lateral durch die Umgebung zu bewegen und ihre Privilegien auszuweiten. Verschärft wird das Problem durch die schiere Anzahl digitaler Identitäten: Nicht-menschliche Identitäten wie Service Accounts, API-Schlüssel und Machine-to-Machine-Verbindungen sind in den meisten Unternehmen inzwischen zahlreicher als menschliche Identitäten. Gleichzeitig werden sie häufig nicht zentral verwaltet und nur selten überprüft. Jede nicht verifizierte Identität und jede unnötige Berechtigung stellt damit ein dauerhaftes Risiko dar.



Abbildung 1: Ablauf eines identitätsbasierten Angriffs

Wenn Identitäten der Ausgangspunkt vieler Angriffe sind, muss auch die Verteidigung bei der Kontrolle von Zugriffen ansetzen. Genau hier kommt das Zugriffsmanagement als operative Ebene der Identity Security ins Spiel: Es überprüft, wer eine Verbindung herstellt, legt fest, wie die Authentifizierung erfolgt, und steuert, welche Aktionen eine Identität ausführen darf – kontinuierlich und nicht nur zum Zeitpunkt der Anmeldung.

Bevor ein Unternehmen über weiterführende Sicherheitsmaßnahmen oder einen höheren Reifegrad seiner Identity Governance sprechen kann, muss dieses Fundament stehen: starke Authentifizierung, Zugriff nach dem Least-Privilege-Prinzip und ein kontrollierter Identity Lifecycle vom Eintritt bis zum Ausscheiden.

2. Herausforderungen für Unternehmen

2.1 Unkontrolliertes Wachstum und Fragmentierung der Identitätslandschaft

Nur wenige Identitätslandschaften sind das Ergebnis einer von Anfang an durchdachten Planung. Vielmehr wachsen sie über Jahre hinweg mit den jeweiligen Anforderungen eines Unternehmens: Hier kommt eine neue Anwendung hinzu, dort eine Cloud-Plattform, und nach einer Übernahme muss plötzlich ein weiteres Verzeichnis mit eigenen Regeln für die Vergabe von Zugriffsrechten integriert werden. Über die Jahre entsteht so ein sogenannter **Identity Sprawl** – eine zunehmend fragmentierte Identitätslandschaft, in der ein und derselbe Mitarbeiter über zahlreiche voneinander unabhängige Konten verfügt, Berechtigungen über verschiedene Systeme verteilt sind und sich selbst eine grundlegende Frage kaum noch zuverlässig beantworten lässt: Wer hat eigentlich Zugriff worauf?



Abbildung 2: Identity Sprawl – ein Mitarbeiter, zahlreiche voneinander unabhängige Konten

Die damit verbundenen Risiken sind hinlänglich bekannt und haben meist dieselbe Ursache: Es fehlt eine zentrale Verwaltung. Beim Deprovisioning müssen Konten in jedem System einzeln deaktiviert werden – mit der Folge, dass Benutzerkonten häufig länger bestehen bleiben als das Beschäftigungsverhältnis der Personen, für die sie ursprünglich eingerichtet wurden. Wechseln Mitarbeiter ihre Rolle, sammeln sich Zugriffsrechte an, weil benötigte Berechtigungen zwar vergeben, anschließend jedoch nur selten überprüft oder wieder entzogen werden. Wer sich mit zahlreichen separaten Logins auseinandersetzen muss, greift zudem schnell auf wiederverwendete Passwörter zurück, da sich eine große Zahl starker, individueller Zugangsdaten kaum praktikabel verwalten lässt.

Gleichzeitig wächst die Zahl nicht-menschlicher Identitäten – darunter Service Accounts, API-Schlüssel, Zugangsdaten für Integrationen, **KI-Agenten und andere Maschinenidentitäten** – schneller als jede andere Kategorie. Sie werden häufig außerhalb des direkten Einflussbereichs der IT angelegt und teilweise über Jahre hinweg mit statischen Zugangsdaten betrieben.

Die Fragmentierung erschwert es zusätzlich, diese Probleme in den Griff zu bekommen. Wird die Authentifizierung in jedem System separat umgesetzt, orientiert sich das tatsächliche Sicherheitsniveau letztlich an der schwächsten Implementierung – eine einzige Legacy-

Anwendung ohne MFA kann bereits ausreichen, um eine Sicherheitslücke zu schaffen. Werden Zugriffsrichtlinien über unterschiedliche Management-Konsolen verwaltet, wird ihre konsistente Umsetzung zur manuellen Aufgabe. Und bei einem Audit müssen die erforderlichen Informationen mühsam aus einzelnen Systemen zusammengetragen werden. Security-Teams sind damit für eine Angriffsfläche verantwortlich, die sie nur teilweise überblicken können – und gerade die Übergänge und Lücken zwischen den Systemen sind für Angreifer besonders interessant.

Hinzu kommt, dass Identity Sprawl kaum in zwei Unternehmen die gleiche Form annimmt. Die meisten IT-Umgebungen sind zwangsläufig hybrid und verbinden Cloud-Anwendungen mit On-Premises-Infrastrukturen. In regulierten Branchen oder Unternehmen mit besonderen Anforderungen an digitale Souveränität kommen zudem Systeme hinzu, die die eigene Infrastruktur überhaupt nicht verlassen dürfen. Eine wirksame Antwort auf die Fragmentierung der Identitätslandschaft muss daher die gesamte Umgebung berücksichtigen – und nicht nur diejenigen Bereiche, die sich besonders einfach anbinden lassen.

2.2 Angriffe auf Zugangsdaten sind professionalisiert und skalierbar geworden

Phishing ist längst keine Aktivität mehr, die nur in kleinem Maßstab oder von hoch spezialisierten Angreifern betrieben wird. Phishing-as-a-Service-Plattformen stellen heute fertige Infrastrukturen bereit, mit denen sich Anmeldeseiten von Unternehmen imitieren, Zugangsdaten abgreifen und einige weit verbreitete Formen der Multi-Faktor-Authentifizierung umgehen lassen. Dienste wie Tycoon 2FA ermöglichen den Einsatz solcher Methoden in großem Maßstab. Dadurch sinkt die technische Einstiegshürde für Angreifer, während fortgeschrittene Phishing-Techniken als kommerziell verfügbare Services angeboten werden.

Eine besonders relevante Entwicklung ist das sogenannte Adversary-in-the-Middle-Phishing (AiTM). Bei einem AiTM-Angriff schaltet der Angreifer einen Proxy zwischen den Benutzer und den legitimen Authentifizierungsdienst. Das Opfer durchläuft den regulären Anmeldeprozess – einschließlich Einmalcode oder Push-Bestätigung –, während der Angreifer das dabei erzeugte Session-Token bzw. Cookie abgreift. Dadurch kann er unter Umständen auf das Konto zugreifen, ohne den Authentifizierungsprozess erneut durchlaufen zu müssen – selbst wenn herkömmliche MFA aktiviert ist. Microsoft meldete für das Jahr 2024 einen Anstieg der beobachteten AiTM-Phishing-Angriffe um 146 %.



Abbildung 3: Ablauf eines Adversary-in-the-Middle-Angriffs – MFA wird durchgeführt und dennoch umgangen

Auch andere MFA-Verfahren haben ihre Grenzen. Push-Benachrichtigungen können durch wiederholte Bestätigungsanfragen missbraucht werden, während Einmalpasswörter in Echtzeit abgefangen oder weitergeleitet werden können. Entscheidend ist daher nicht allein, ob MFA eingesetzt wird, sondern ob das verwendete Authentifizierungsverfahren tatsächlich phishing-resistent ist. Methoden, die auf gemeinsamen Geheimnissen, Codes oder einer Bestätigung durch den Benutzer beruhen, bieten ein deutlich anderes Schutzniveau als kryptografische Verfahren wie FIDO2-Sicherheitsschlüssel und Passkeys.

Der Missbrauch gestohlener Zugangsdaten bleibt dennoch ein wichtiger Angriffsweg in Unternehmensumgebungen. Laut dem Verizon Data Breach Investigations Report 2026 entfielen 13 % der beobachteten Initial-Access-Aktivitäten auf gestohlene Zugangsdaten. Verschaffen sich Angreifer über eine legitime Identität Zugang, können ihre Aktivitäten zunächst denen eines autorisierten Benutzers ähneln. Verdächtiges Verhalten lässt sich dadurch erheblich schwerer von normalen Aktivitäten unterscheiden.

2.3 Regulatorischer Druck

Regulierungsbehörden in allen wichtigen Märkten stellen zunehmend dieselbe Anforderung: Unternehmen müssen kontrollieren können, wer Zugriff auf ihre Systeme hat – und diese Kontrolle auch nachweisen können. In Europa weitet NIS2 die

Cybersicherheitsanforderungen auf zusätzliche Branchen aus. Zu den Maßnahmen, die betroffene Organisationen gegebenenfalls umsetzen müssen, gehören auch Zugriffskontrollen und Multi-Faktor-Authentifizierung. Gleichzeitig verpflichtet DORA Finanzunternehmen zu einer stärkeren Governance von IKT-Risiken – einschließlich Zugriffskontrollen, privilegierter Konten und Zugriffe durch Dritte. Die DSGVO verlangt weiterhin einen angemessenen Schutz personenbezogener Daten. Eine nachvollziehbar dokumentierte Access Governance, regelmäßige Überprüfungen von Berechtigungen und die zeitnahe Deaktivierung nicht mehr benötigter Konten sind daher wichtige Compliance-Maßnahmen.

Auch außerhalb Europas zeigt sich eine vergleichbare Entwicklung. In den USA verlangen SOX und HIPAA in ihren jeweiligen Anwendungsbereichen nachweisbare Zugriffskontrollen, während Zero-Trust-Vorgaben auf Bundesebene Behörden und deren Dienstleister zunehmend in Richtung phishing-resistenter MFA führen. In Großbritannien ergänzen die dort geltende UK GDPR, die Vorgaben der FCA zur Operational Resilience und Cyber Essentials einander; Zugriffskontrollen und MFA sind dadurch auch für viele Geschäfte mit dem öffentlichen Sektor von Bedeutung. Im Nahen Osten entwickeln sich Datenschutzgesetze wie Saudi-Arabiens PDPL kontinuierlich weiter, während Regulierungsbehörden wie die SAMA konkrete Anforderungen an das Identity Management im Finanzsektor stellen. Eine ähnliche Entwicklung zeigt sich im asiatisch-pazifischen Raum – von Japans APPI und Singapurs PDPA bis hin zu den MAS-Vorgaben für privilegierte Zugriffe. Über nationale Regelwerke hinaus begleiten Standards wie PCI DSS und ISO 27001 Unternehmen über Ländergrenzen hinweg und machen Access Management damit nicht nur zu einer regulatorischen, sondern zunehmend auch zu einer vertraglichen Anforderung.



Abbildung 4: Unterschiedliche Regelwerke, eine gemeinsame Anforderung

Jedes dieser Regelwerke hat seinen eigenen Geltungsbereich und Zeitplan. In ihrer Gesamtheit weisen sie jedoch in dieselbe Richtung: Identity- und Access-Kontrollen sind längst keine rein interne Sicherheitsentscheidung mehr, sondern eine externe Anforderung – und Unternehmen müssen jederzeit in der Lage sein, deren Umsetzung nachzuweisen.

2.4 Die Falle mangelnder Benutzerfreundlichkeit

Sicherheitsmaßnahmen, die im Arbeitsalltag zu viele Hürden schaffen, werden häufig umgangen. Ständige Authentifizierungsaufforderungen verleiten Benutzer dazu, nach Abkürzungen zu suchen. Komplexe Passwortanforderungen führen dazu, dass Passwörter wiederverwendet, nach vorhersehbaren Mustern abgewandelt oder unsicher gespeichert werden. Langwierige Prozesse für die Beantragung von Zugriffsrechten erhöhen wiederum die Wahrscheinlichkeit, dass Zugangsdaten geteilt oder unkontrollierte Workarounds genutzt werden.

Dabei geht es nicht allein um die Disziplin der Benutzer, sondern um die Gestaltung der Prozesse. Zugriffssicherheit für Mitarbeiter ist dann am wirksamsten, wenn der sicherste Weg zugleich der einfachste ist. Benutzer sollten sich einmal authentifizieren, auf die für ihre Rolle erforderlichen Anwendungen zugreifen, schnellere und sicherere Authentifizierungsverfahren als Passwörter nutzen und alltägliche Zugriffsanforderungen ohne unnötige Verzögerungen

erledigen können. Eine Lösung, die Benutzerfreundlichkeit nur als zweitrangig betrachtet, fördert auf Dauer genau die Verhaltensweisen, die sie eigentlich verhindern soll.



Abbildung 5: Komplexe Prozesse fördern genau das Verhalten, das sie verhindern sollen – deshalb gilt es, unnötige Hürden zu beseitigen

3. Wo der Handlungsdruck am größten ist

Diese Herausforderungen betreffen die meisten Organisationen. Besonders ausgeprägt sind sie jedoch in Branchen, in denen komplexe Umgebungen, sensible Systeme und hohe regulatorische Anforderungen zusammentreffen.

Öffentlicher Sektor und Verwaltung

Öffentliche Verwaltungen betreiben große und heterogene Anwendungslandschaften – von modernen Cloud-Diensten bis hin zu Systemen, die bereits seit Jahrzehnten im Einsatz sind. Auf diese Systeme wird über Ministerien, Behörden und Kommunen hinweg zugegriffen, häufig unter strengen Anforderungen an Auditierbarkeit, digitale Souveränität und die Kontrolle darüber, wo Identitätsdaten gespeichert werden.

Für diese Organisationen kommt es darauf an, eine einheitliche Authentifizierung über die gesamte Anwendungslandschaft hinweg zu gewährleisten, starke Authentifizierungsverfahren entsprechend den geltenden Anforderungen des öffentlichen Sektors einzuführen und sämtliche Zugriffsaktivitäten vollständig und unter eigener Kontrolle nachweisen zu können.

4. Was eine Identity-Access-Lösung leisten muss

Eine wirksame Lösung für den sicheren Mitarbeiterzugriff sollte fünf zentrale Funktionen bieten.



Abbildung 6: Fünf Kernfunktionen einer Lösung für sicheren Mitarbeiterzugriff

4.1 Einheitlicher und nahtloser Zugriff auf die gesamte Anwendungslandschaft

Die Grundlage bildet Single Sign-On (SSO) für Cloud- und On-Premises-Anwendungen. Benutzer authentifizieren sich über einen zentralen Zugangspunkt und erhalten Zugriff auf die für ihre jeweilige Rolle freigegebenen Anwendungen, ohne für jede Anwendung ein separates Passwort verwalten zu müssen.

Dadurch reduziert sich die Zahl der im Umlauf befindlichen Zugangsdaten, der Aufwand für Passwort-Resets sinkt und IT-Teams erhalten einen zentralen Ansatzpunkt, um Richtlinien durchzusetzen und Zugriffe zu überwachen. Gleichzeitig gewinnt die zentrale Authentifizierungsebene an Bedeutung. Da sie den Zugang zu mehreren Anwendungen absichert, muss sie besonders geschützt, hochverfügbar und kontinuierlich überwacht werden.

4.2 Authentifizierung, die modernen Angriffsmethoden standhält

Bei der Multi-Faktor-Authentifizierung müssen Benutzer Faktoren aus unterschiedlichen Kategorien vorweisen – beispielsweise etwas, das sie wissen, etwas, das sie besitzen, oder ein biometrisches Merkmal. Dies erschwert die Kompromittierung von Konten erheblich. Das tatsächliche Schutzniveau hängt jedoch maßgeblich davon ab, welche Faktoren zum Einsatz kommen.

Einmalpasswörter können abgefangen oder in Echtzeit weitergeleitet werden. Push-Benachrichtigungen können durch wiederholte Authentifizierungsanfragen oder Social Engineering missbraucht werden. Bei Adversary-in-the-Middle-Angriffen kann eine legitime Authentifizierungssitzung über einen Proxy geleitet und das dabei erzeugte Session-Token abgegriffen werden – selbst wenn bestimmte Formen von MFA aktiviert sind. Der Einsatz von MFA allein garantiert daher noch keinen Schutz vor Phishing.

Phishing-resistente Authentifizierungsverfahren setzen genau an dieser Schwachstelle an. FIDO2- und WebAuthn-Verfahren, darunter Hardware-Sicherheitsschlüssel und Passkeys, binden die Authentifizierung mithilfe von Public-Key-Kryptografie an den legitimen Dienst. Es gibt weder einen wiederverwendbaren Code noch ein Shared Secret, das ein Benutzer versehentlich auf einer gefälschten Website preisgeben könnte. Zertifikatsbasierte Authentifizierungsverfahren, beispielsweise mit Smartcards, bieten einen vergleichbaren Schutz und sind in Behörden, im Verteidigungsbereich und anderen Umgebungen mit besonders hohen Sicherheitsanforderungen weiterhin weit verbreitet.



Abbildung 7: MFA ist nicht gleich MFA – wie gut gängige Verfahren vor Phishing schützen

Auch regulatorische und technische Empfehlungen berücksichtigen diesen Unterschied zunehmend. Die ANSSI empfiehlt kryptografische Authentifizierungsverfahren, wenn ein höheres Sicherheitsniveau erforderlich ist, und warnt davor, sich bei Einmalcodes auf schwächere Übertragungskanäle zu verlassen. Die CISA bezeichnet phishing-resistente MFA – einschließlich FIDO/WebAuthn und PKI-basierter Authentifizierung – als bevorzugten

Standard. Auch europäische Leitlinien zur Umsetzung von NIS2 weisen Unternehmen bei sensiblen Zugriffen zunehmend in Richtung phishing-resistenter Verfahren.

Die Einführung sollte risikobasiert erfolgen. Administratoren, privilegierte Benutzer und Personen mit Zugriff auf kritische Systeme sollten zunächst priorisiert werden. Anschließend kann die Nutzung schrittweise ausgeweitet werden, soweit Geräte und Arbeitsabläufe dies zulassen. Die Lösung sollte diesen Übergang über ein einheitliches Policy-Framework unterstützen, anstatt eine sofortige unternehmensweite Migration vorauszusetzen.

4.3 Föderation auf Basis bestehender Infrastruktur – ohne grundlegende Migration

Unternehmen haben über Jahre hinweg in ihre Verzeichnisinfrastruktur investiert. Active Directory und LDAP bilden die maßgebliche Quelle dafür, welche Mitarbeiter wo tätig sind und welche Rollen sie innehaben, und sind eng mit Prozessen in HR, IT und Security verknüpft. Eine Lösung für den sicheren Mitarbeiterzugriff, die eine Abkehr von dieser bestehenden Grundlage voraussetzt, dürfte daher bereits bei der Evaluierung auf erhebliche Hürden stoßen.

Gefragt ist vielmehr **Föderation**: Die Lösung nutzt bestehende Verzeichnisse weiterhin als maßgebliche Identitätsquellen, synchronisiert sich mit ihnen und erweitert deren Reichweite über Standardprotokolle auf weitere Anwendungen. Dazu gehören SAML und OpenID Connect für moderne Webanwendungen, RADIUS für Netzwerkgeräte und Infrastruktur sowie SCIM für die automatisierte Benutzerbereitstellung in kompatiblen Diensten. Bestehende Identitäten, Gruppen und Organisationsstrukturen bleiben erhalten. Gleichzeitig wird die gesamte Anwendungslandschaft über eine zentrale Authentifizierungsebene erreichbar – einschließlich Systemen, die ursprünglich nicht für eine Föderation ausgelegt wurden.



Abbildung 8: Föderation erweitert bestehende Verzeichnisdienste über Standardprotokolle

Dieser Ansatz ermöglicht zudem eine realistische Umsetzung innerhalb regulatorisch vorgegebener Fristen. Verbindliche Compliance-Termine lassen keinen Spielraum für mehrjährige Migrationen von Verzeichnisdiensten. Eine Lösung, die auf der bestehenden Infrastruktur aufsetzt, kann dagegen innerhalb weniger Monate eine starke Authentifizierung über die gesamte Anwendungslandschaft hinweg ermöglichen.

4.4 Identity Lifecycle ohne manuellen Verwaltungsaufwand

Jede Identität durchläuft einen Lebenszyklus – vom Eintritt über Rollenwechsel bis zum Ausscheiden. In jeder dieser Phasen besteht das Risiko, dass die tatsächlich vergebenen Zugriffsrechte unbemerkt von den vorgesehenen Berechtigungen abweichen. Eine geeignete Lösung muss es daher ermöglichen, den gesamten Identity Lifecycle zentral zu verwalten: Konten werden vom ersten Tag an mit den zur jeweiligen Rolle passenden Zugriffsrechten eingerichtet, Berechtigungen bei Rollenwechseln entsprechend angepasst und beim Ausscheiden eines Mitarbeiters sämtliche Zugriffe gleichzeitig entzogen. Zentral angewendete gruppen- und rollenbasierte Richtlinien ersetzen dabei die separate Administration auf Anwendungsebene.

Damit lassen sich zwei typische Schwachstellen manueller Administration vermeiden: die schleichende Anhäufung von Berechtigungen (Privilege Creep) und verwaiste Konten, die nach dem Ausscheiden ihrer ursprünglichen Besitzer weiterhin bestehen. Gleichzeitig wird aus einem wiederkehrenden operativen Aufwand ein kontrollierter Prozess: Eine Person verfügt genau über die Zugriffsrechte, die ihrer jeweiligen Rolle entsprechen – jederzeit nachvollziehbar und nachweisbar.

4.5 Integrierte Nachweise für Audits

Alle in diesem Dokument behandelten regulatorischen Vorgaben laufen letztlich auf dieselben Fragen hinaus: Wer hat Zugriff worauf? Wie wird dieser Zugriff abgesichert? Und lässt sich dies auch nachweisen? Eine Lösung für den sicheren Mitarbeiterzugriff muss diese Fragen auf Basis ihrer eigenen Daten beantworten können – durch vollständige Authentifizierungsprotokolle, eine aktuelle Übersicht der Benutzer und ihrer jeweiligen Anwendungsberechtigungen sowie ein Reporting, das nicht nur für Administratoren, sondern auch für Auditoren geeignet ist. Durch die Integration mit SIEM-Plattformen lassen sich identitätsbezogene Ereignisse zudem in die übergeordneten Detection- und Response-Prozesse des Unternehmens einbinden.

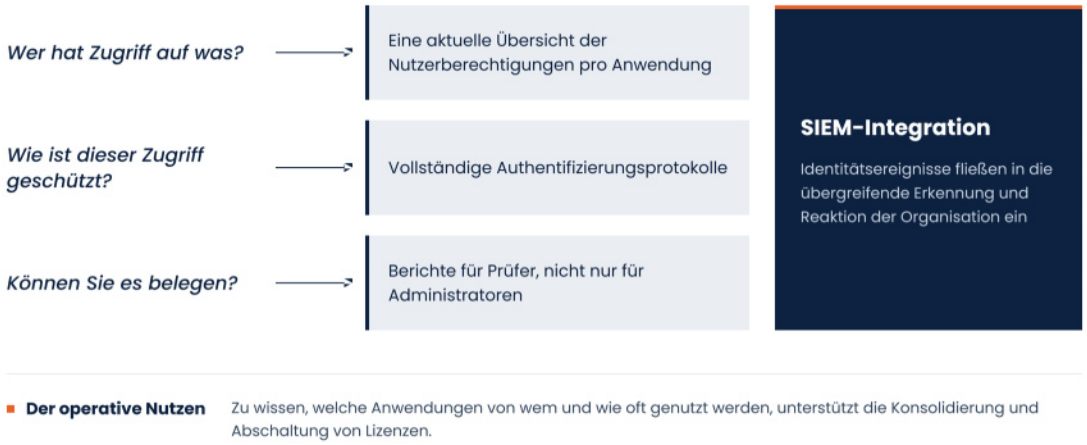


Abbildung 9: Die drei zentralen Fragen des Auditors – beantwortet anhand der Daten der Lösung

Diese Transparenz bietet über Compliance-Anforderungen hinaus auch einen operativen Mehrwert: Erkenntnisse darüber, welche Anwendungen tatsächlich genutzt werden, von wem und wie häufig, liefern IT-Teams eine fundierte Grundlage, um Lizenzbestände zu optimieren und nicht mehr benötigte Anwendungen außer Betrieb zu nehmen.

5. Eine Plattform – Ihr Betriebsmodell

Die zuvor beschriebenen Funktionen definieren, **was** eine Lösung für den sicheren Mitarbeiterzugriff leisten muss. Die Frage, **wo** sie betrieben wird, ist davon unabhängig und richtet sich nach dem regulatorischen Umfeld, der bestehenden Infrastruktur und dem Risikoprofil des jeweiligen Unternehmens.

Als Service (SaaS). Der schnellste Weg zur Nutzung der benötigten Funktionen: Es muss keine eigene Infrastruktur bereitgestellt werden, Betrieb und Updates übernimmt der Anbieter und die Skalierung erfolgt flexibel im Hintergrund. Dieses Modell eignet sich für Unternehmen, die ihre Zugriffssicherheit innerhalb weniger Wochen produktiv einsetzen möchten und die Lösung als Service beziehen wollen, anstatt sie selbst zu betreiben.

Als On-Premises-Appliance. Die gleichen Funktionen werden innerhalb der eigenen Infrastruktur des Unternehmens bereitgestellt. Identitätsdaten, Authentifizierungsprozesse und Protokolle verbleiben vollständig unter der Kontrolle des Unternehmens – innerhalb der eigenen Infrastruktur, des geltenden Rechtsraums und der eigenen operativen Verantwortung. Dieses Modell eignet sich insbesondere für Organisationen mit hohen Anforderungen an digitale Souveränität, für regulierte Ausschreibungen, die cloudbasierte

Über WALLIX

WALLIX (Euronext: ALLIX, seit 2015) ist ein Cybersecurity-Anbieter und europäischer Marktführer im Bereich Privileged Access Management (PAM). Das Unternehmen unterstützt Organisationen dabei, ihre digitale Souveränität zu sichern und ihre Handlungsfreiheit in einer zunehmend vernetzten Welt zu bewahren.

Die technologische Leistungsfähigkeit der WALLIX One Plattform, die von führenden Analystenhäusern anerkannt wird, unterstützt weltweit bis zu 4.000 Organisationen bei ihrer Sicherheitsstrategie. Die Mission von WALLIX ist klar: Identitäten, Zugriffe und Privilegien in IT- und OT-Umgebungen zu schützen – und dabei Effizienz, Einfachheit und Compliance miteinander zu verbinden, damit Unternehmen sich sicher und frei in einer zunehmend digitalen Welt weiterentwickeln können.

WWW.WALLIX.COM

wallix