Mehr Sicherheit auf dem Mac mit Cloud Identity

Neue Möglichkeiten in einem digitalem Arbeitsumfeld.

Jahrelang fuhren Mitarbeiter ins Büro, starteten ihren Computer, meldeten sich mit ihrem Benutzernamen und ihrem Passwort im Unternehmensnetzwerk an und legten mit ihrer täglichen Arbeit los.

Heute wird jedoch zunehmend seltener zu den üblichen Geschäftszeiten und ausschließlich im Büro gearbeitet. Eine Untersuchung von Gallup ergab, dass 43 Prozent der Mitarbeiter in den USA außerhalb des Büros arbeiten.[1] Diese wachsende Anzahl mobiler Mitarbeiter benötigt jedoch denselben sicheren Zugriff auf Ressourcen wie ihre Kollegen im Büro – und das ohne Verbindung zum Unternehmensnetzwerk. Darüber hinaus müssen beide Mitarbeitergruppen in der Lage sein, die zunehmende Anzahl von in der Cloud bereitgestellten Apps und Ressourcen sicher zu nutzen. Um diesen Anforderungen gerecht zu werden, sind einige Anpassungen hinsichtlich der in Unternehmen eingesetzten Technologien und IT-Konzepte erforderlich.

Der erste Schritt um Mitarbeiter moderne Tools an die Hand zu geben, die sie für das heutige Arbeitsleben benötigen, ist die Einführung von Mitarbeiterprogrammen zur Geräteauswahl. Auf diese Weise kann jeder Mitarbeiter selbst bestimmen, ob er lieber mit einem PC oder einem Mac arbeiten möchte. Da sich immer mehr Mitarbeiter für einen Mac entscheiden, benötigt die IT-Abteilung eine maßgeschneiderte Lösung, mit der sie Geräte und Benutzer schützen kann, ganz gleich, wo sie sich gerade befinden.

In diesem White Paper werden neue und bessere Möglichkeiten aufgezeigt, wie Sie Ihre Benutzer, Ihre Macs und die darauf befindlichen Daten sowie das Unternehmen überhaupt mithilfe eines cloudbasierten Identity Provider bestmöglich schützen.

Moderne Authentifizierung auf dem Mac

Zwar haben Technologien wie Active Directory (AD) und Lightweight Directory Access Protocol (LDAP) bei der Authentifizierung auf dem Mac in den vergangenen Jahren gute Dienste geleistet, jedoch sind sie den Anforderungen heutiger moderner Umgebungen immer weniger gewachsen.

Deshalb sind Benutzer gezwungen, auf old-school Verfahren zurückzugreifen, um Zugang zu internen Ressourcen zu erhalten. Dazu gehört die Nutzung eines unternehmenseigenen Local Area Network (LAN) oder eines Virtual Private Network (VPN) – beides Möglichkeiten, die ein suboptimales Benutzererlebnis bieten. Bei Verwendung des Plug-Ins für Active Directory können Benutzer beispielsweise nur dann ihr Passwort ändern, wenn der Active Directory Dienst erreichbar ist. Das führt häufig zu Verwirrung und teuren Support-Tickets beim Helpdesk.

Durch diese umständlichen Konzepte ergeben sich zwei wesentliche Herausforderungen:

1. Verschwendete IT-Ressourcen
Wenn Mitarbeiter außerhalb des Büros arbeiten, sind sie nicht automatisch mit dem Unternehmensnetzwerk verbunden. Das führt zu Problemen im Zusammenhang mit Passwörtern. Laut einem Bericht von Gartner beziehen sich 40 Prozent der beim Helpdesk eingereichten Support-Tickets auf das Zurücksetzen von Passwörtern.[2] Viele dieser Tickets stammen von Mitarbeitern, die außerhalb des Büros tätig sind und ihre Passwörter vergessen haben.

Jedes eingereichte Ticket verursacht Kosten. Nach Angaben von Gartner belaufen sich die Kosten für eine Anfrage beim Helpdesk auf durchschnittlich 17,88 US-Dollar.[2] Und wenn die IT-Aufgaben an externe Stellen auslagern, müssen für jedes Ticket häufig sogar enorme Pauschalbeträge gezahlt werden, selbst wenn ein Passwort nur zurückgesetzt werden soll.

Diese Tickets und Kosten summieren sich schnell. Allein für das Zurücksetzen von Passwörtern können unnötige Ausgaben von mehreren tausend Euro entstehen.

2. Höhere Sicherheitsrisiken
Wenn Sie Active Directory, LDAP oder Kerberos als primäre Tools für die Benutzerauthentifizierung nutzen, lassen sich Konzepte wie die Multi-Faktor-Authentifizierung oder die Verbesserung der Sicherheit durch hardwarebasierte Mechanismen nur äußerst schwer umsetzen.

In einem Bericht von iPass wird als größte Bedrohung für die Sicherheit von Unternehmensdaten die zunehmende Mobilität der Mitarbeiter genannt. Tatsächlich vermuten 57 Prozent der weltweit befragten CIOs und Entscheidungsträger in IT-Abteilungen, dass ihre mobilen Mitarbeiter im vergangenen Jahr gefährdet waren oder selbst ein Sicherheitsrisiko darstellten.[3]

Lokale Tools erfüllen nicht alle Anforderungen

Bislang war Microsoft Active Directory in Bezug auf das lokale Identitäts- und Accountsmanagement das Maß aller Dinge. Mit Active Directory sind Daten und Anwendungen in Unternehmen vor Zugriffen durch alle Personen geschützt, die keine Mitarbeiter sind und deshalb nicht im Verzeichnis enthalten sind.

Obwohl Active Directory in der Vergangenheit bei den meisten Unternehmen zur Lösung von Authentifizierungsproblemen zum Einsatz kam, wird es heutigen Anforderungen nicht mehr gerecht.

Warum?

Da in Unternehmen statt PCs immer mehr Macs verwendet werden, hinterfragen die IT-Verantwortlichen die bewährten Verfahren, die bislang für die Integration von Mac Computern in Active Directory galten.

Tatsächlich ergeben sich für externe Mitarbeiter, die sich mit Active Directory authentifizieren, zurzeit mehrere Probleme im Hinblick auf Sicherheit und Benutzerfreundlichkeit:

1. Für die Authentifizierung mit Active Directory müssen sich die Mitarbeiter in der Domäne befinden. Das ist bei externen Mitarbeiter jedoch nicht möglich.

2. In der Vergangenheit war Active Directory der Identitätsdienst der Wahl, allerdings bieten heute viele Arbeitgeber ihren Mitarbeitern die Möglichkeit, mit einem Mac zu arbeiten. Das geht mit einem Kontrollverlust für externe Apple Benutzer und eingeschränkten Funktionen für die

Benutzerverwaltung einher. Um Abhilfe zu schaffen, wird auf Add-ons von Drittanbietern zurückgegriffen, die jedoch die Benutzerverwaltung erschweren und höhere Kosten verursachen.

3. IT-Administratoren können keine Befehle und Skripte in Form von Richtliniendokumenten bereitstellen, mit denen die gewünschten Einstellungen für die Computer und Benutzer innerhalb ihres Kontrollbereichs übernommen werden.

Die Bindung an eine Active Directory Domäne war 20 Jahre lang eine großartige Lösung, um Authentifizierungsprobleme zu umgehen. Auch jetzt bietet es noch eine geeignete Lösung, doch in einer Welt mit immer mehr mobilen Geräten ist die Synchronisierung von Passwörtern und Uhrzeiten oftmals schwierig, Einträge im Domain Name System sind nicht immer extern verfügbar und Active Directory ist nicht mehr die bestmöglichste Lösung.

Alte IT-Systeme und -Prozesse sind ebenfalls keine Option. Heutige Mitarbeiter wollen immer und überall mit einem Höchstmaß an Sicherheit und Benutzerfreundlichkeit produktiv sein können.

Wie können Sie also eine Bindung an Active Directory bei Mac Geräten vermeiden und gleichzeitig die Accountsicherheit gewährleisten? Mit einem cloudbasierten Identitätsdienst (Identity Management).

Einführung zu cloudbasierten Identitätsdiensten

Ohne die richtigen Tools kann die Sicherheit auf Remote-Geräten nicht gewährleistet werden. Demzufolge muss der Ansatz für Identität und Sicherheit neu durchdacht werden. Mit einem Cloud-Identitätsanbieter, wie z. B. Microsoft, Google, Okta, IBM und OneLogin, in Kombination mit Security Assertion Markup Language (SAML) und Open Authorization (OAuth) können Sie Ihre Umgebung neu gestalten.

Was ist eine Cloud-Identität?

Mithilfe einer Cloud-Identität kann die IT-Abteilung Benutzer und Benutzergruppen sowie deren Zugang zu Unternehmensanwendungen und Cloud-Ressourcen sowohl zentral als auch per Fernzugriff verwalten.

> **Bedenkt man, dass in 81 Prozent der Unternehmen Multi-Cloud-Umgebungen zum Einsatz kommen und 26 Prozent der Unternehmen mehr als 6 Millionen US-Dollar pro Jahr für eine Public-Cloud-Infrastruktur ausgeben, ist es schwieriger als jemals zuvor, in Bezug auf Identität und Sicherheit nicht ins Hintertreffen zu geraten.[4]**

Dementsprechend legt Microsoft Unternehmen den Wechsel von einer lokalen Active Directory Bereitstellung hin zu einer cloudbasierten Lösung mit Microsoft Azure Active Directory nahe.

Mit den Cloud-Diensten von Microsoft Azure können Unternehmen Anwendungen mithilfe spezifischer Tools und Frameworks in einem stabilen, globalen Netzwerk erstellen, verwalten und bereitstellen. Die Lösung wird von 95 Prozent der Fortune 500 Unternehmen eingesetzt.4

Microsoft Azure ist jedoch nicht der einzige cloudbasierte Identitätsdienst. Stattdessen haben Unternehmen die Qual der Wahl. Für welche(n) Anbieter sollen sie sich entscheiden?

Jamf Connect für die Integration in cloudbasierte Identitätsdienste

Mit Jamf Connect spielt es keine Rolle, welchen cloudbasierten Identitätsdienst Sie nutzen. Jamf Connect ermöglicht eine einfache Benutzereinrichtung mit Multi-Faktor-Authentifizierung über einen cloudbasierten Identitätsdienst im Rahmen eines Apple Einrichtungsworkflows:

Auf diese Weise können für alle lokalen Benutzer flexibel dieselben, durch einen Verzeichnis- oder Identitätsdienst bereitgestellten Richtlinien und Kontrollmechanismen durchgesetzt werden.

Mithilfe von Jamf Connect kann ein Benutzer seinen Mac Computer auspacken, einschalten und nach einmaliger Anmeldung mit Anmeldeinformationen für den jeweiligen cloudbasierten Identitätsdienst sofort verwenden, um auf seine Unternehmensanwendungen zuzugreifen.

Daraus ergeben sich mehrere Vorteile:

1. SICHERER REGISTRIERUNGSPROZESS: Dank moderner Authentifizierungsverfahren können Sie sicher sein, dass sich der richtige Benutzer am Gerät anmeldet, bevor Sie sensible Ressourcen darauf bereitstellen.

2. SPONTANE ACCOUNTERSTELLUNG: Erstellen Sie nach Bedarf lokale Accounts basierend auf Identitäten von Okta, Azure, Google Cloud, IBM Cloud und OneLogin.

3.CLOUDBASIERTE MULTI-FAKTOR-AUTHENTIFIZIERUNG: Profitieren Sie bei der Benutzeranmeldung von unterstützten Verfahren für die Multi-Faktor-Authentifizierung mit Okta, Azure, Google Cloud, IBM Cloud oder OneLogin.

Sie verwenden eine lokale Lösung?

Dann ist NoMAD für Sie die richtige Wahl. Nutzen Sie das volle Potenzial Ihrer Mac Computer mithilfe von NoMAD, einer Lösung zur nahtlosen Synchronisierung von Accounts in Umgebungen, in denen Active Directory verwendet wird.

Mobile Device Management (MDM) und bedingter Zugriff

Da Organisationen zunehmend auf die cloudbasierte Lösung von Active Directory umsteigen und vermehrt Mac Computer bereitstellen, ist der Schutz ihrer Unternehmensdaten oberstes Gebot. Dadurch darf jedoch nicht das erstklassige Benutzererlebnis beeinträchtigt werden, für das Apple bekannt ist.

Durch die Integration eines cloudbasierten Identitätsdiensts in Jamf Connect können IT-Administratoren Benutzer, Passwörter und den Zugriff auf Unternehmensanwendungen aus der Ferne verwalten. Auf diese Weise können Unternehmen sicher sein, dass

ihre Daten auch in der heutigen von Mobilität geprägten Geschäftswelt stets geschützt sind.

In Kombination mit einem Workflow für die automatische Registrierung in der MDM-Lösung ist der gesamte Prozess denkbar einfach.

1. Der Benutzer wird eingeladen, sein Gerät mithilfe der automatischen Registrierung in der MDM-Lösung zu registrieren.

2. Während des Registrierungsvorgangs wird das Jamf Connect Paket vom MDM-Server heruntergeladen und auf dem Gerät installiert.

3. Anschließend wird sofort das Anmeldefenster von Jamf Connect angezeigt. Es muss kein eigener Account mit separaten Anmeldeinformationen erstellt werden.

Der Benutzer benötigt nur einen Benutzernamen und ein Passwort und profitiert von einem fantastischen Benutzererlebnis, ohne sich Gedanken um die Accountsicherheit machen zu müssen.

Tatsächlich ermöglichen Sie mit der richtigen, eigens für Apple Geräte entwickelten MDM-Lösung allen Mitarbeitern, sei es im Büro oder auf der anderen Seite des Globus, die erwartete automatische Einrichtung ohne großen manuellen Konfigurationsaufwand.

Wir helfen Ihnen

Wir unterstützen Sie tatkräftig dabei, Ihre Umgebung zu schützen und die Anzahl von Support-Tickets zu senken, die wegen Problemen mit Passwörtern eingereicht werden. Kontaktieren Sie uns noch heute, um mit uns die nächsten Schritte für mehr Sicherheit auf Ihren Apple Geräten zu besprechen.

Lassen Sie Jamf Ihre Herausforderungen rund um die Benutzerauthentifizierung meistern.

Kontaktieren Sie uns noch heute für die ersten Schritte. Gerne können Sie Jamf Connect zunächst kostenlos testen und sich von den Integrationsmöglichkeiten für cloudbasierte Identitätsdienste überzeugen.

Jetzt kontaktieren **Testversion anfordern**

Gerne können Sie sich auch an einen autorisierten Händler für Apple Geräte Ihrer Wahl wenden, um Jamf Connect zu testen.

QUELLEN:
1: http://news.gallup.com/reports/199961/7.aspx#aspnetForm
2: Gartner Document #G00258742
3: https://www.ipass.com/mobile-security-report/
4: https://www.rightscale.com/lp/state-of-the-cloud

jamf

www.jamf.com/de

Um zu sehen wie auch Ihr Unternehmen mit Jamf Connect modernere Arbeitsprozesse implementieren kann, besuchen Sie **www.jamf.com/de.**