DATENBLATT

Starling Two-Factor Authentication

Sichere und einfache Identitätsverifizierung

Vorteile

- Höhere Sicherheit für nahezu alle Systeme und Anwendungen
- Einfache, fortlaufende Verwaltung, da keine Infrastrukturkosten und weiteren Komplexitäten anfallen, die mit lokalen Lösungen einhergehen
- Einfacher Umstieg dank Angebot benutzerfreundlicher Authentifizierungsoptionen wie Authentifizierung per Tastendruck, SMS oder Anruf
- Ermöglichung schneller Reaktion des Helpdesks auf Probleme bei der Benutzerauthentifizierung von jedem beliebigen Webbrowser
- Geringeres Risiko eines Sicherheitsverstoßes aufgrund kompromittierter oder gestohlener Authentifizierungsdaten
- Bereitstellung eines umfangreichen Audit Trails zur Einhaltung gesetzlicher Bestimmungen

Überblick

Eine Kompromittierung von Kennwörtern wirkt sich negativ auf den Ruf und das Geschäftsergebnis des Unternehmens aus, unabhängig davon, wie Kennwörter kompromittiert werden, ob durch fragwürdiges Benutzerverhalten, Verwendung schwacher Kennwörter oder Diebstahl von Kennwörtern. Mit der Zwei-Faktor-Authentifizierung für den Zugriff auf Ihre Netzwerkressourcen können Sie problemlos für mehr Sicherheit sorgen und Datensicherheitsverletzungen vermeiden.

Mit Starling Two-Factor Authentication, einer SaaS-basierten Lösung, können Sie Ihr Unternehmen schützen, höhere Produktivität von Benutzern gewährleisten und erheblich die Menge der Helpdesk-Anrufe für die Zurücksetzung von Kennwörtern reduzieren.

Sicherer und einfacher Benutzerzugriff

Die einfache und sicherste Möglichkeit zur Lösung dieses Kennwortproblems ist die Zwei-Faktor-Authentifizierung. Zwei-Faktor-Lösung ist jedoch nicht gleich Zwei-Faktor-Lösung. Sie sollten überlegen, wie die Betriebsabläufe in Ihrem Unternehmen sind, wie Authentifizierungsprozesse effizienter gestaltet werden können, welche Tokenformfaktoren benötigt werden und was für den vorhandenen Anwendungsstack und die vorhandene Infrastruktur in Frage kommt.

Starling Two-Factor Authentication löst das Kennwortproblem, ohne die Investitionskosten zu verursachen, die im Zusammenhang mit herkömmlichen Vor-Ort-Lösungen entstehen. Dank des benutzerfreundlichen Dashboards für Administratoren und der flexiblen Authentifizierungsoptionen für Endbenutzer können Unternehmen die Identität eines Benutzers schnell und einfach prüfen.

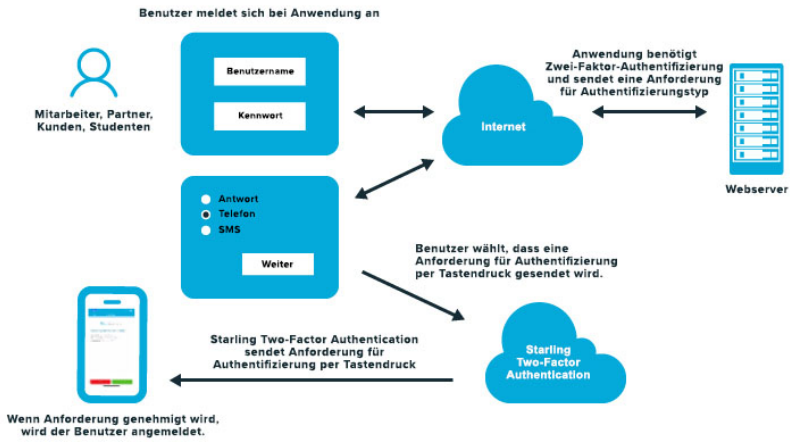

Abbildung 1. Starling Two-Factor Authentication-Architektur und -module.

Funktionen und Merkmale

Benutzerfreundliches Dashboard für Administratoren

Durch das rollenbasierte Dashboard für Administratoren mit Genehmigungsworkflow wird sichergestellt, dass Administratoren und Helpdesk-Mitarbeiter die passenden Aufgaben und Rechte erhalten. Gleichzeitig wird die Verwaltung von Endbenutzerkonten, die Generierung von temporären Antwortcodes und das Ausführen von Health Checks zur Verifizierung der ordnungsgemäßen Funktion der mobilen App erleichtert.

Mehrere Authentifizierungsmethoden

Benutzer können mit der mobilen Starling 2FA-App für iOS, Android und Chrome Einmalkennwörter generieren oder sich ein Einmalkennwort per SMS oder Telefonanruf übermitteln lassen.

Authentifizierung per Tastendruck

Gestalten Sie die Zwei-Faktor-Authentifizierung für Ihre Benutzer noch einfacher: Sie können das Einmalkennwort überspringen und die Authentifizierung per Tastendruck wählen, indem sie ihren Benutzernamen und ihr Kennwort in einer Anwendung eingeben. Anschließend wird eine SMS-Verifizierung an ihre mobile App übermittelt, die es ihnen ermöglicht, den Anmeldeversuch zu gewähren oder abzulehnen. Sobald die Genehmigung erfolgt ist, werden sie automatisch bei der Anwendung angemeldet.

Token

Starling Two-Factor Authentication bietet verschiedene Optionen, einschließlich mobiler Apps für iOS, Android und Chrome sowie SMS und Anrufe.

Token-Branding

Über das Starling Dashboard können Administratoren problemlos das Aussehen des Tokens in der mobilen App an das Unternehmens-Branding anpassen.

ADFS Adapter

Dieser Adapter ermöglicht Organisationen die Implementierung von Zwei-Faktor-Authentifizierung in Anwendungen, die das Microsoft WS-Federation Protokoll nutzen, wie z. B. Office 365. Außerdem ist das System mit weiteren Federation-Protokollen kompatibel, einschließlich SAML 2.0 mit Unterstützung für Support-Anmeldungen bei Cloud-Anwendungen wie Google Apps oder salesforce.com.

RADIUS-Agent

Dieser Adapter erlaubt es Organisationen, die Zwei-Faktor-Authentifizierung auf allen Geräten zu unterstützen, die das RADIUS-Protokoll für die Authentifizierung nutzen.

HTTP Agent

Schützen Sie IIS-Websites mit Zwei-Faktor-Authentifizierung.

Desktop-Anmeldung

Verbessern Sie Ihre Umgebung, indem Sie den Computern und Servern von Benutzern durch Vereinheitlichung von Benutzeranmeldungen und gestärkte Authentifizierung Zwei-Faktor-Authentifizierung hinzufügen.

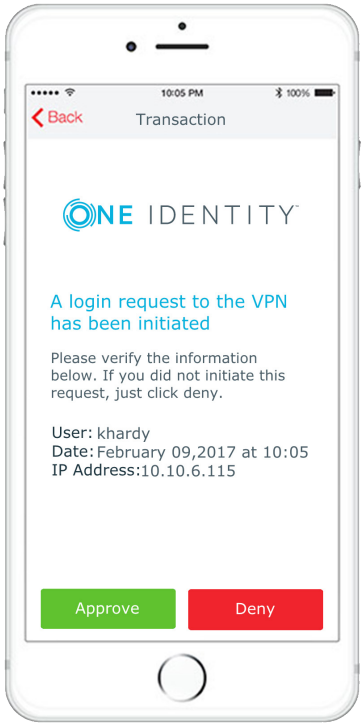

Abbildung 2. Die Authentifizierung per Tastendruck sorgt für eine einfachere und sichere Benutzeranmeldung.

Über One Identity

One Identity unterstützt Unternehmen bei der erfolgreichen Umsetzung von Identitäts- und Zugriffsmanagement (IAM). Mit unserem einzigartigen Portfolio an Lösungen für Identity Governance, Zugriffsverwaltung, Verwaltung privilegierter Konten und Identity-as-a-Service-Lösungen können Organisationen ihr volles Potenzial entwickeln, ohne Einschränkung durch Sicherheit, und profitieren dabei vom Schutz vor Bedrohungen. Weitere Informationen finden Sie unter OneIdentity.com.