

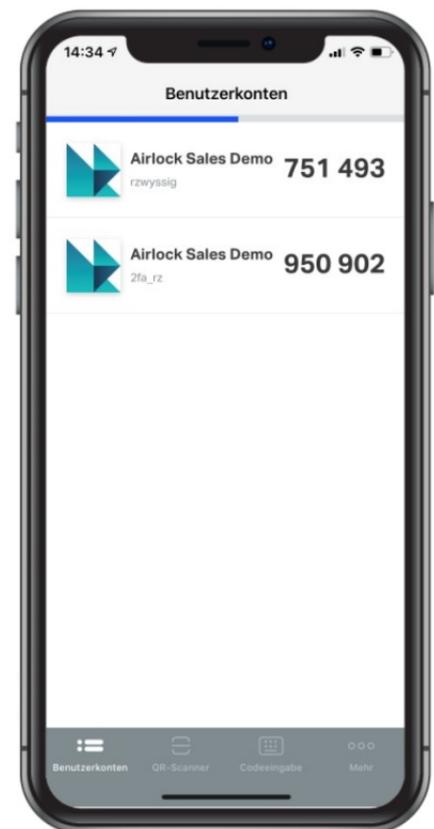
# Zwei-Faktor-Authentifizierung ohne Aufwand

Dr. Götz Güttich

*Mit 2FA bietet Airlock (eine Security Innovation der Ergon Informatik AG) eine Lösung zur Zwei-Faktor-Authentifizierung, die dabei hilft, Benutzerkonten in Unternehmensumgebungen besser abzusichern, als das allein mit Benutzername und Passwort möglich ist. Diese zusätzliche Sicherheit muss im heutigen Arbeitsalltag unbedingt gewährleistet werden, leider bringt eine Zwei-Faktor-Authentifizierung aber immer erhöhten Aufwand für die Anwender mit und gilt deshalb in der Praxis als unbeliebt. Airlocks 2FA mit Zero-Touch-Authentifizierung soll hier mit seiner einfachen Bedienung Abhilfe schaffen. Das Produkt konnte im Testlabor seine Leistungsfähigkeit unter Beweis stellen.*

Airlock bietet mit IAM (Identity and Access Management) eine zentrale Authentisierungsplattform für Unternehmen an. Diese unterstützt eine große Zahl an Authentifizierungsverfahren, wie zum Beispiel Zwei-Faktor-Authentifizierung (2FA) mit mTAN, OATH oder auch E-Mail und automatisiert die Benutzeradministration. Da die Self-Service-Funktionalität besonders leistungsfähig ist können die Anwender den größten Teil der mit der Verwaltung ihrer Konten zusammenhängenden Tätigkeiten selbst erledigen, was das Help-Desk und die IT-Abteilung entlastet.

Airlock 2FA wurde nahtlos in das IAM-Produkt integriert und erweitert die eben genannten Zwei-Faktor-Authentifizierungsmethoden wie mTAN und OATH um eine zusätzliche Option. Damit wendet sich Airlock vor allem an drei Zielgruppen: Unternehmen, die eine eigene 2FA-Umgebung aufbauen wollen, Unternehmen die ihre bestehende 2FA-Infrastruktur (zum Beispiel auf Basis



von SecurID) modernisieren möchten und Unternehmen, die 2FA für ihre Kunden und Mitarbeiter besonders einfach gestalten wollen. Die Verwaltung der Benutzer, die Authentifizierungsmethoden und das Management sämtlicher Schlüssel laufen im Betrieb über IAM ab.

In der Praxis lassen sich dann mit dem Produkt Zugriffe auf Home-Offices, Online-Services, Schnittstellen, Portale, VPNs und Web-Anwendungen absichern. Es handelt sich bei IAM also um eine vorgelagerte Authentifizierungslösung, die die Zugriffe auf die gesamte Applikationslandschaft

eines Unternehmens schützt und das separate Sichern einzelner Anwendungen überflüssig macht. Bei Bedarf ist es sogar möglich, mit dem System Banktransaktionen zu bestätigen.

## Der Funktionsumfang von Airlock 2FA

Bei Airlock 2FA handelt es sich um einen Cloud-basierten Service, der zusammen mit dem Airlock-Gateway und der genannten IAM-Lösung zum Einsatz kommt. Kunden können diesen Dienst optional zu den genannten Airlock-Produkten dazu buchen. Um 2FA zu nutzen, müssen aber der Gateway und die IAM-Lösung bereits vorhanden sein.

Ein besonderes Highlight von Airlock 2FA ist das Zero-Touch-Feature. Dieses macht ein sicheres Einloggen ohne weitere Benutzerinteraktion möglich und soll damit dafür sorgen, dass der Login-Prozess genauso einfach abläuft, wie bei Konten, die nur mit Username und Passwort abgesichert werden. Wie das genau funktioniert, werden wir später im Test noch zeigen.

Abgesehen davon ermöglicht die zu Airlock 2FA gehörende App auch einen Login via Passcode, also einen alle 30 Sekunden erzeugten Sicherheits-Code. Die 2FA läuft dann so wie beispielsweise über den Google Authenticator. Um Anforderungen wie PSD2 zu erfüllen, unterstützt das Produkt, wie gesagt, auch Transaktionsbestätigungen.

Abgesehen davon besteht auch die Option, passwortlose Anmeldungen möglich zu machen. Das eliminiert den Einsatz unsicherer Passwörter und steigert die Benutzerfreundlichkeit. Bei einem

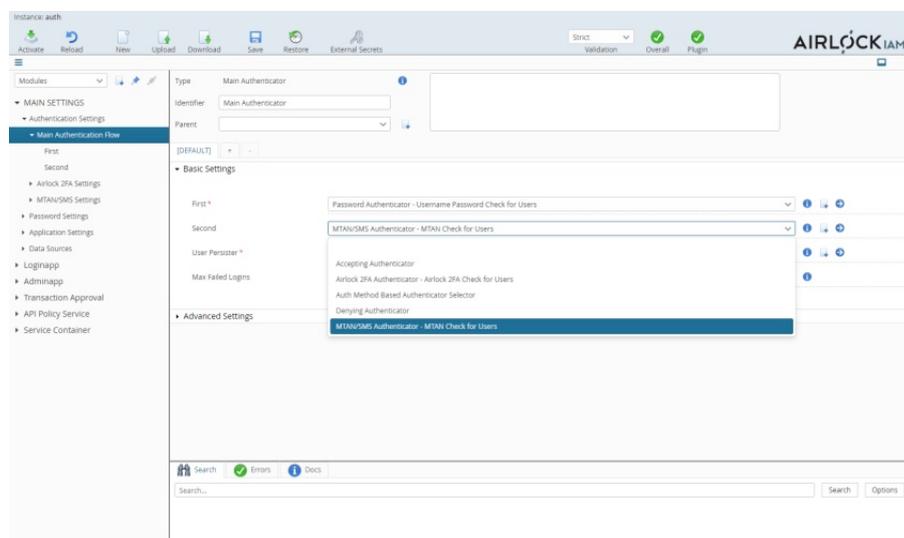
passwortlosen Login kann die Authentifizierung beispielsweise über One-Touch, also eine Anmeldung mit Benutzererkennung ohne Passwort und einen Fingerabdruck, einen PIN oder via Gesichtserkennung auf dem Smartphone erfolgen.

## Der Test

Im Test verwendeten wir eine Demo-Umgebung mit einem Testunternehmen namens "Virtinc", dessen Benutzer über unterschiedliche Authentifizierungsmethoden auf die Virtinc-Online-Assets (in

thenticator anmeldete. Alle diese Authentifizierungsverfahren werden von Airlocks IAM-Lösung out of the box unterstützt, so dass es keine Schwierigkeiten dabei gab, entsprechende Benutzerkonten anzulegen.

Nach dem Login konnten die Anwender in unserer Testumgebung auf das erwähnte Wordpress-Blog von Virtinc zugreifen und zwar als Administrator und als User. Unsere Aufgabe im Test war es nun, die genannten Benutzerkonten auf Airlock 2FA umzustellen,



**Als einer der ersten Schritte bei der Migration zu Airlock 2FA ist es erforderlich, die zweite Authentifizierungsmethode umzustellen**

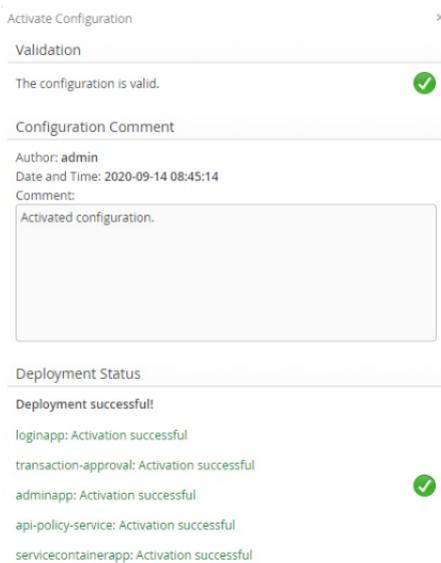
der Testumgebung handelte es sich dabei um ein Wordpress-Blog) zugegriffen. Konkret arbeiteten wir dabei mit der zum Testzeitpunkt aktuellen Versionen der IAM-Lösung (7.2.1).

Die für den Test erzeugten Benutzerkonten setzten unterschiedliche Authentifizierungsmethoden ein. Dazu gehörten einmal ein einfacher Login per Passwort, außerdem verwendeten wir auch Zwei-Faktor-Authentifizierungen mit Codes per E-Mail und mTAN (SMS). Dazu kam zusätzlich noch ein Nutzerkonto, das sich via OATH über den Google-Au-

so dass sie genau wie zuvor weiterarbeiten konnten, nur eben statt der jeweils vorher verwendeten Authentifizierungsmethode mit 2FA. Dazu stellte uns Airlock Zugangsdaten für den Cloud-basierten "Futurae"-Server zur Verfügung, über den 2FA abgewickelt wird.

Wir richteten damit unser System administratorseitig so ein, dass es 2FA einsetzte und stellten die Benutzerkonten dann so um, dass sie innerhalb einer vorgegebenen Zeitspanne von den Anwendern selbst auf das neue Authentifizierungssystem migriert wurden.

Die eigentliche Arbeit des Umstellens übernehmen in der Praxis also die User selbst, die im Laufe dieses Prozesses auch gleich über die Migration und die damit ver-



**Zum Abschluss der IAM-Konfiguration muss das aktuelle Setting noch aktiviert werden**

bundenen Konsequenzen informiert werden.

Im Rahmen des Tests nahmen wir zunächst einmal den bei der Umstellung anfallenden Arbeitsaufwand unter die Lupe, und zwar sowohl für die Administratoren als auch für die User, die ihre Konten mit Hilfe der Self-Service-Funktionen selbst migrierten. Zum Schluss sahen wir uns die Funktionsweise von Airlock 2FA im laufenden Betrieb an, testeten das Zero-Touch-Feature für den kontaktlosen Login und analysierten unsere Ergebnisse.

### Die Implementierung von 2FA in unserer Testumgebung: Arbeiten auf Administratorseite

Um die Lösung in Betrieb zu nehmen, loggten wir uns zunächst einmal beim IAM-Konfigurationswerkzeug ein, um die Konfiguration auf Administratorseite vorzunehmen. Sobald das erledigt war, wechselten wir nach

“Konfiguration / MAIN SETTINGS / Authentication Settings / Airlock 2FA Settings / Futuræ Server”. Dort war es nötig, die Service ID, den Authentication API Key und den Administration API Key für den Futuræ-Server einzutragen (diese Informationen hatten wir im Vorfeld von Airlock erhalten) und anschließend die geänderte Konfiguration zu aktivieren.

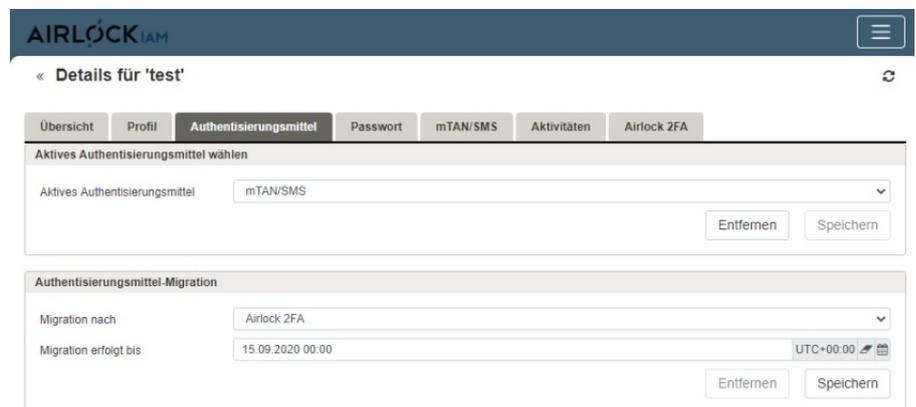
“Konfiguration / MAIN SETTINGS / Authentication Settings / Main Authentication Flow” und stellten dort unter den “Basic Settings” unter “Second” als zweite Authentifizierungsmethode die Option “Auth Method Based Authenticator Selector” ein. Diese sorgt dafür, dass die Administratoren dazu in die Lage versetzt werden, für jeden Anwender einen spezifischen zweiten Faktor zu definieren.

Im zweiten Schritt geht es zunächst darum, das Plugin "Airlock 2FA Settings" in die Konfiguration einzubinden. Das geht ebenfalls über den Eintrag "Authentication Settings" unter "MAIN SETTINGS".

Im Rahmen der Installation des Plugins müssen die zuständigen Mitarbeiter dann noch die verwendete Datenbank und das

MAIN SETTINGS / Authentication Settings / Airlock 2FA Settings / Futuræ Server”. Dort war es nötig, die Service ID, den Authentication API Key und den Administration API Key für den Futuræ-Server einzutragen (diese Informationen hatten wir im Vorfeld von Airlock erhalten) und anschließend die geänderte Konfiguration zu aktivieren.

Im Laufe des Einsatzes von Airlock 2FA werden in der Datenbank verschiedene Informationen abgelegt, die beim Löschen des betroffenen Anwenders wieder gelöscht werden müssen. Für diese Aufgabe steht der "User Change Listener" zur Verfügung, der sich unter "Data Sources / User Data Source / User Change Event Listeners" einrichten lässt. Er heißt "Airlock 2FA Consistency User Change Listener" und wird als Plugin unter "User



**Im letzten Schritt auf Administratorseite ist es jetzt noch erforderlich, die Migration anzustoßen**

Default-Plugin für die Verschlüsselung auswählen. Das geht in den meisten Fällen – so auch bei uns – über eine Selektion aus einer Drop-Down-Liste heraus. Anschließend wechseln die Administratoren nach “Konfiguration /

Change Event Listeners" aktiviert.

Zum Schluss bereiteten wir jetzt unsere Test-Benutzerkonten auf die Migration vor. Dazu wechselten wir im IAM-Konfigurations-

interface nach “Benutzer”, riefen den ersten User-Eintrag auf und wechselten nach “Authentisierungsmittel”.

Hier fanden wir einen Bereich namens “Authentisierungsmittel-Migration” vor. Dort gaben wir an, dass die Migration nach “Airlock 2FA” stattfinden sollte und legten einen Termin fest, bis zu

**Bevor der Anwender sein Konto auf Airlock 2FA umstellen kann, muss er sich erst einmal mit seiner alten Authentifizierungsmethode einloggen**

dem die Migration durchgeführt werden musste, beispielsweise zwei Wochen später.

Mit den genannten Arbeitsschritten war nun alles erledigt, was auf Administratorseite erforderlich war. Die restliche Arbeit übernehmen anschließend die Anwender selbst. Es besteht übrigens auch die Option, mehrere oder alle Benutzerkonten im Unternehmen auf die gleiche Weise parallel zu migrieren. Auf diese Art und Weise ist auch eine stufenlose Migration im Mischbetrieb möglich, was das ganze Vorgehen deutlich vereinfacht und viel Arbeit sparen kann.

**Die auf Anwenderseite erforderlichen Migrationsschritte**

Um nun die eigentliche Migration durchzuführen, wechselten wir nun auf die Anwenderseite.

Zunächst einmal installierten wir auf unserem Huawei Mate 20-Smartphone die Airlock-2FA-App, die für Android und iOS verfügbar ist. Sie unterstützt Touch ID mit Fingerabdruck, Face ID (Gesichtserkennung) sowie Authentifizierungen via PIN.

Falls gewünscht, lässt sich bei der App auch ein Branding mit eigenem Logo durchführen, alternativ besteht sogar die Option, eine kundenspezifische App mit individuell gestaltetem Look and Feel bereit zu stellen. Zusätzlich stehen für Umgebungen ohne Smartphones auch Hardware-Tokens mit Display und Kamera zur Verfügung. Nach der Installation der App loggten wir uns mit dem eben vorbereiteten Benutzerkonto (dieses arbeitete mit dem mTAN-Verfahren als zweitem Authentifizierungsschritt) auf der Virtinc-Webseite ein. Daraufhin landeten wir nicht auf der üblichen Benutzerseite mit den Zugriffsoptionen auf das zuvor erwähnte Wordpress-Blog.

Statt dessen machte uns das System darauf aufmerksam, dass ein Wechsel auf Airlock 2FA erforderlich war und dass dieser Wechsel bis zu einem bestimmten Termin durchgeführt werden musste. Zu diesem Zeitpunkt hat der Anwender dann die Wahl, auf “Jetzt umstellen” zu klicken und die Migration durchzuführen oder “Später umstellen” zu selektieren und dann normal weiterzuarbeiten.

Im Test führten wir zu diesem Zeitpunkt die Migration durch. Daraufhin bot uns das System an, mit der App einen QR-Code zu scannen und einen Namen für das Mobilgerät zu vergeben. Sobald wir das erledigt hatten, erschien

in unserer App der neu eingerichtete Zugriff mit Logo, Namen und einem ständig wechselnden Zahlen-Token, das man, wie vom Google Authenticator her bekannt, als zweites Authentifizierungselement beim Anmelden bei der Webseite benutzen kann, aber – wie wir gleich noch sehen werden – in den meisten Fällen nicht muss.

Dass die Registrierung des Endgeräts erfolgreich war, sieht man übrigens auch im Log beziehungsweise im Admin-Portal, in dem das Mobilgerät im Airlock-2FA-Reiter des dazugehörigen Benutzerkontos aufgeführt wird. Der Anwender sollen sich nun ausloggen und neu anmelden. Bei der ersten Anmeldung ist es erforderlich, den Login in der App auf dem Smartphone manuell zu erlauben. Das geht entweder über die Eingabe des eben erwähnten Zahlen-Tokens oder über die bereits beschriebene One-Touch-

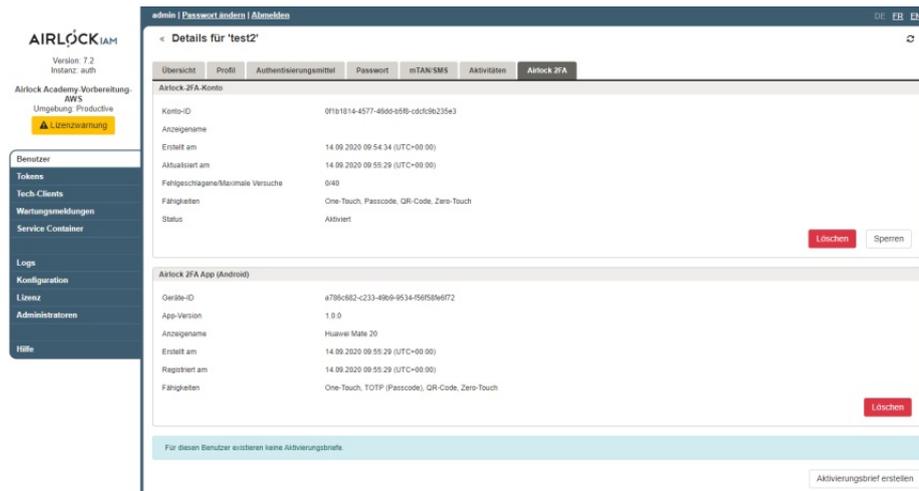
**Nach erfolgreichem Login bietet das System die Migration an**

Funktion. Danach kann man dann normal mit dem Online-Dienst arbeiten, für den man sich authentifiziert hat, in diesem Falle dem Blog von Virtinc.

**Zero-Touch macht die Arbeit mit dem Smartphone überflüssig**

Sobald die Migration abgeschlossen wurde, ist es auf Android-Systemen möglich, bei den folgenden Logins mit der Zero-

Touch-Funktion zu arbeiten. Diese funktioniert folgendermaßen: und erlaubt die Anmeldung, wenn es sich um den richtigen



Das über den QR-Code registrierte Gerät erscheint unter anderem auch im Airlock-2FA-Reiter in der Benutzerkontendefinition

Nach dem Login des betroffenen Benutzers mit Username und Passwort führen sowohl der auf dem PC oder Notebook verwendete Browser als auch das Mobilgerät einen Sound-Fingerprint via Mikrofon durch.

Der Browser überträgt denn seinen Sound-Fingerprint an das Smartphone, dieses gleicht die Fingerprints ab und erlaubt den Login, wenn sie übereinstimmen. Auf diese Art und Weise stellt das System sicher, dass sich Smartphone und Rechner am gleichen Ort befinden, ohne dass der Anwender dazu irgendwelche Schritte unternehmen muss.

Das funktioniert gut mit Smartphones, Tablets und Notebooks, da diese in der Regel über ein Mikrofon verfügen. Bei Desktops ist das nicht immer der Fall. Deswegen verfügt Zero-Touch noch über eine Fallback-Funktion, die in Umgebungen zum Einsatz kommt, in denen der PC kein Mikrofon hat. In diesem Fall erzeugt der Desktop-Rechner über seine Lautsprecher einen für Menschen nicht hörbaren Hochfrequenzton. Das Smartphone fängt diesen ab

und handelt. Auch dabei ist keine Benutzerinteraktion erforderlich.

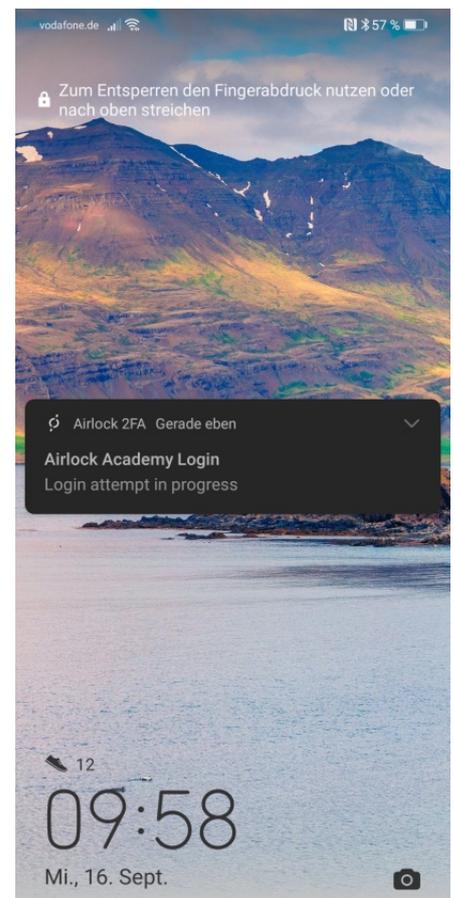
Im Test funktionierten beide Optionen einwandfrei. Sollte es einmal nicht klappen (während des Tests hielten wir mit einem Finger das Mikrofon des Smartphones zu, um das zu überprüfen), besteht immer noch die Möglichkeit, den Login mit dem Token oder einem Fingerabdruck manuell zu genehmigen. Nach dem erfolgreichen Arbeiten mit Zero Touch stellten wir nun die anderen Test-Accounts, die mit den bereits erwähnten weiteren Authentifizierungsmethoden arbeiten, auf Airlock 2FA um. Das funktionierte analog zu dem eben beschriebenen Vorgehen, so dass wir an dieser Stelle nicht weiter darauf eingehen müssen. Es genügt zu sagen, dass alles ohne Schwierigkeiten und mit minimalem Aufwand von Seiten des Administrators über die Bühne ging.

### Zusammenfassung und Fazit

Airlock 2FA konnte uns im Test vor allem mit der Zero-Touch-Funktion überzeugen. Sie macht das Arbeiten mit der Zwei-Faktor-Authentifizierungslösung ge-

nauso einfach, wie einen traditionellen Login mit Benutzernamen und Passwort. Das wird sich sicher positiv auf die Akzeptanz des Produkts im laufenden Betrieb und damit auch auf das Sicherheitsniveau im Allgemeinen auswirken.

Auch die Migration an sich lässt keine Wünsche offen. Die Administratoren müssen lediglich wenige vorbereitende Schritte in der IAM-Konfiguration durchführen, anschließend leitet das System die Anwender von sich aus Schritt für Schritt durch den Migrationsprozess. Aus Kundensicht spricht also nichts gegen den Einsatz dieser Lösung und das Help-



Ein Smartphone während des Zero-Touch-Logins

desk wird wenig belastet. IT-Verantwortliche, die nach einer leistungsfähigen 2FA-Lösung Ausschau halten, werden bei Airlock definitiv fündig.