nevis®
Making security an experience.

Account Takeover: **Identitätsdiebstahl und Betrug** als reelle Bedrohung

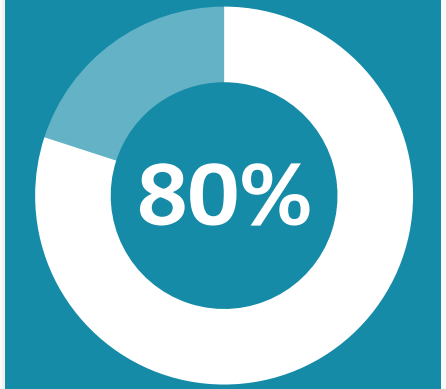
Holger Hinzmann
Head of Channel Sales Europe
Nevis Security GmbH

Anerkannte Qualität: **Unsere Kunden**

BRACK.CH

die Mobiliar

Nevis protects



of all Swiss e-banking transactions

SFS

ETAT DE FRIBOURG
STAAT FREIBURG

EQUATEX

PostFinance

SIX

Helsana

GENERALI

QUILVEST

swisscom

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL

helvetia

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

UBS

ZURICH

Kanton Zug

HIN

VIESMANN

MediData

Gartner: CX Wins!

“Jeder 5. Kunde wechselt nach einem einzigen schlechten Erlebnis **sofort den Anbieter.”**

Quelle: Gartner CX Summit London

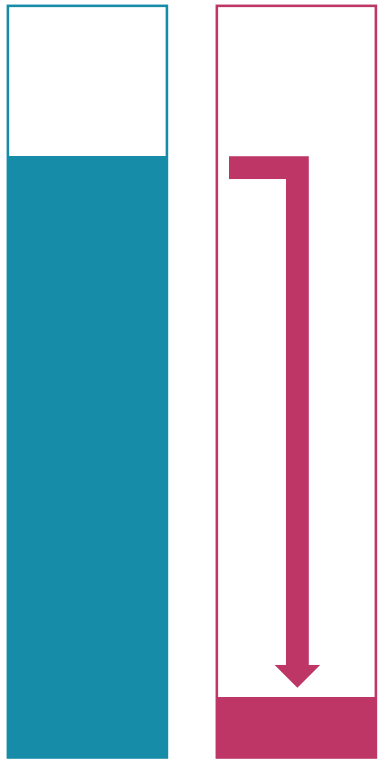
19%

Experience Gap

Die Experience Gap ist die Diskrepanz zwischen Selbsteinschätzung und tatsächlicher Wahrnehmung beim Kunden.

80%

der CEOs glauben, ihre Firma liefert eine hervorragende Experience



8%

der Kunden stimmen zu

+ Good Experience

Kunden mit einer positiven Customer Experience haben eine 3.5x so hohe Bereitschaft einen zusätzlichen Kauf zu tätigen als jene mit einer schlechten Kundenerfahrung.

- Bad Experience

Nach nur einer schlechten Experience mit einem Unternehmen, geben 22% der Konsumenten in Zukunft weniger aus.

Die Hürden für den Endanwender

Wussten Sie, dass...

…Anwender bis zu 130 digitale Benutzerkonten haben?

…Anwender 12 Tage ihres Lebens damit verbringen, nach ihren Benutzernamen und Passwörtern zu suchen?

...weltweit 1 von 3 Online-Transaktionen aufgrund fehlender Benutzer-**namen und Passwörter** abgebrochen wird?

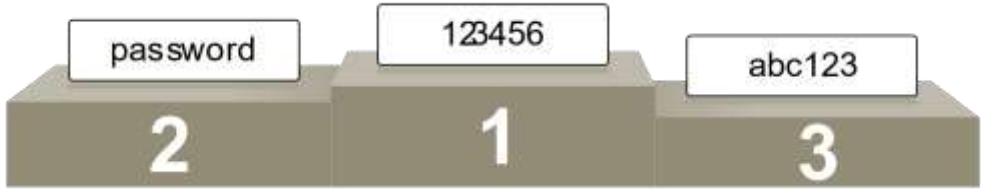
„Passwörter verursachen eine gewisse Frustration beim Nutzer und sind daher ein Hindernis für Ihr digitales Geschäft!"

Die Sicherheits-probleme mit **Passwörtern**

Frühere Passwortregeln führten zu schlechten User-Angewohnheiten:

- Die meisten Passwörter sind **kürzer als 10 Zeichen**
- 52% der Anwender benutzen **dieselben Passwörter für** mehrere Benutzerkonten
- Mehr als 80% der erfolgreichen Datenschutzverletzungen erfolgen mittels Brute Force oder dem Einsatz gestohlener oder verlorener Zugangsdaten

Lieblingspasswörter:



Praktisch, aber nicht sicher! Verbreitete Passwörter:

32 %

Fantasiewörter
Leider leicht zu knacken

21 %

Geburtstag oder Haustiernamen

11 %

Lange, sichere Sätze
Sicher, aber selten genutzt

Bequem, aber nicht sicher – **Mehrfach genutzte Passwörter**

52 %

Nutzen ein Passwort für mehrere Websites

13 %

Haben nur ein Passwort für alles

Quelle: Verizon Data Breach Investigations Report 2020

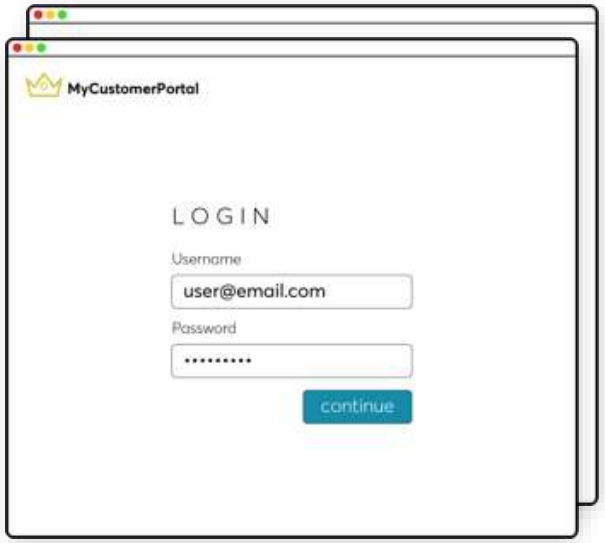
Die Methoden der Angreifer…

1 Mio Accounts

Combolist

Erfolgsrate 0.5 – 3%

Kompromitierte Accounts: 5'000 – 30'000



Gestohlene Passwörter

- Pishing- oder Malware
- Data leaks (e.g Marriot, LinkedIn, Equifax, etc.)
- Can be baught in the darknet
- Often used passwords

Optimierte Tools für spezifische Ziele

- Bank Accounts
- Cloud Storage
- Gaming, Betting and Gambling
- Airlines and Hotels
- Dating Portale
- E-Commerce Accounts

Attackierte Websites

- Bank Accounts
- Cloud Storage
- Gaming, Betting and Gambling
- Airlines and Hotels
- Dating Portals
- etc…

Die gute Nachricht:

Es gibt eine Lösung!

„Setzen Sie auf passwortlose Authentisierung: Das Ersetzen von Passwörtern durch biometrische Authentisierung kann *sowohl die Benutzerfreundlichkeit als auch die Sicherheit verbessern* – eine Kombination, die es bei Sicherheits- und IAM-Tools nicht oft gibt."

Gartner:
2020 Planning Guide for Identity
and Password Management

Die Lösung im Überblick

Passwortfrei - Stress vorbei

Alle Kanäle
Alle Geräte

FIDO UAF und FIDO2

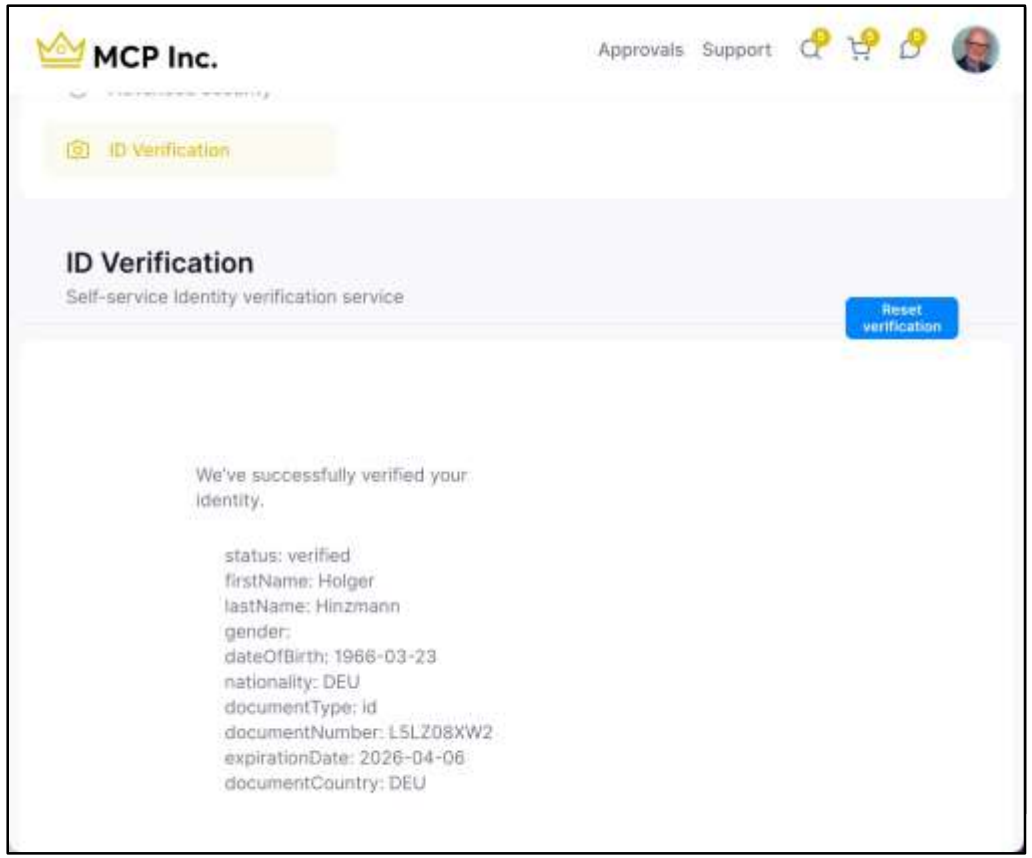
Passwortfreie Authenticator App im Kunden-Branding iOS & Android

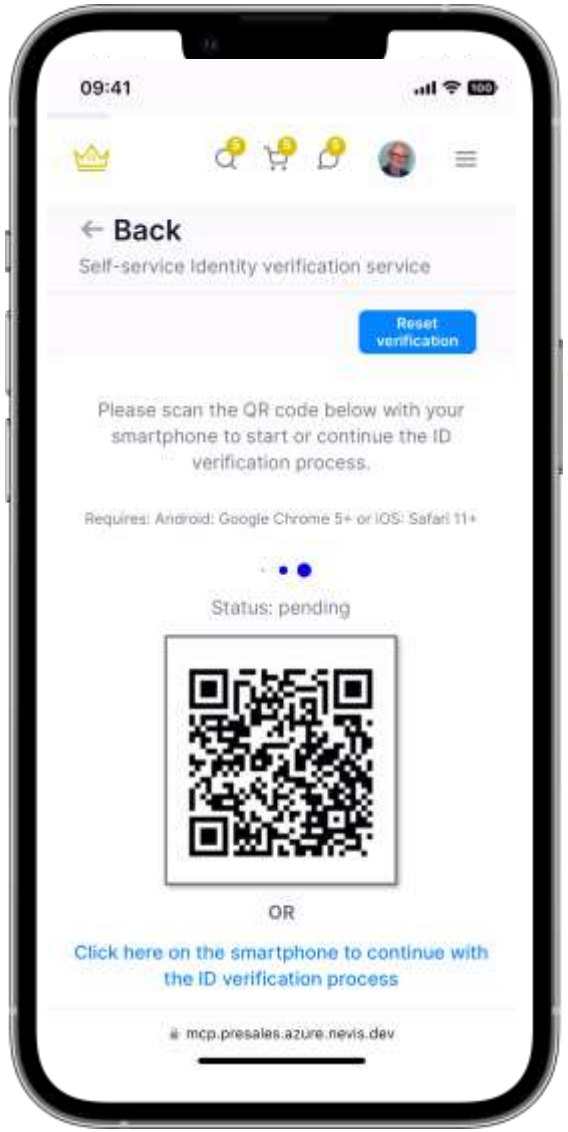
Integration von Passwortfreie Authentisierung in eine bestehende Mobile App mittels SDK for iOS & Android

Passwortfreie Authentisierung mittels Browser (ohne App) FIDO2 / WebAuthN

Benutzersicht:
Die User Journey

Schutz vor New Account Fraud: ID Verifikation

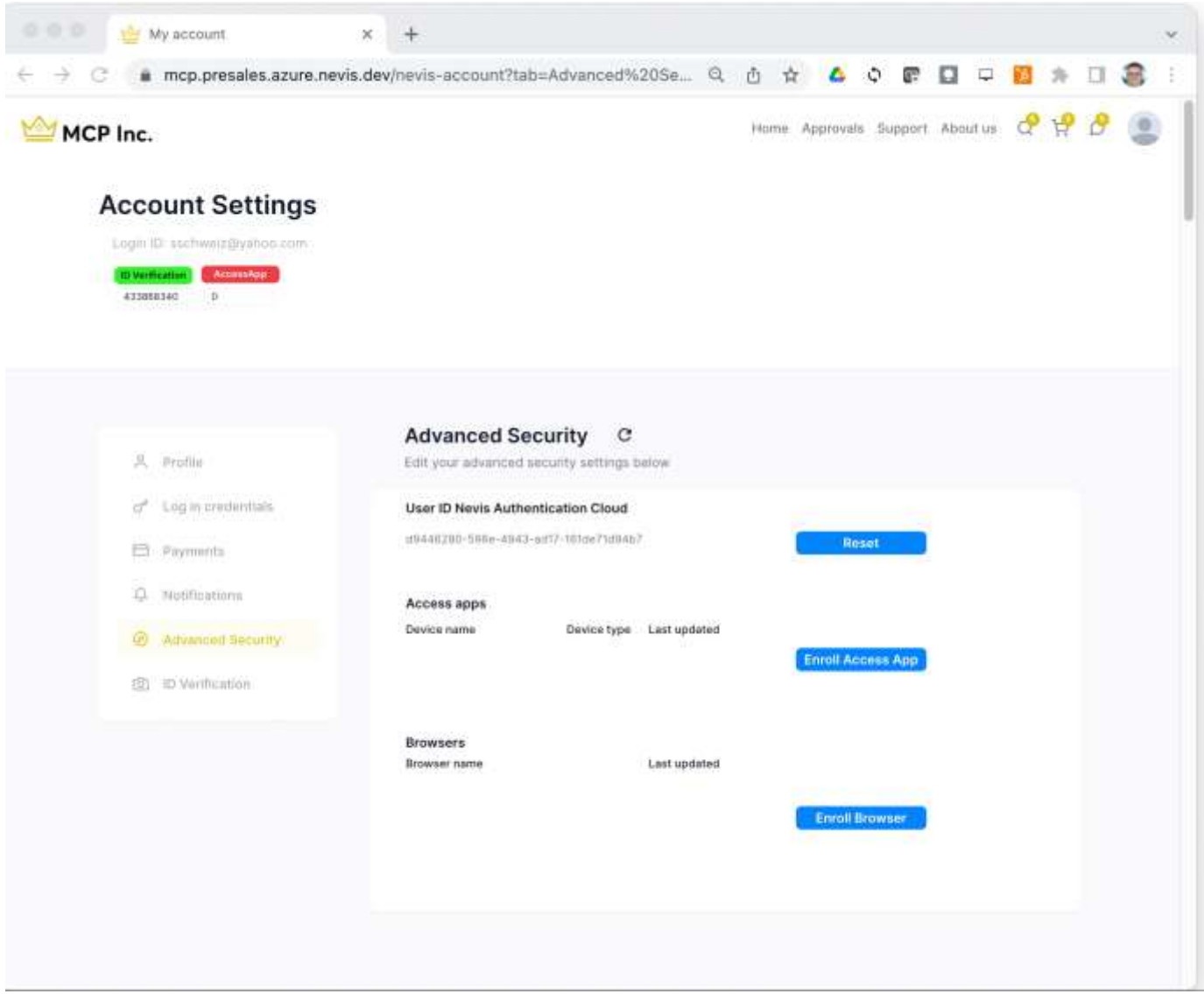




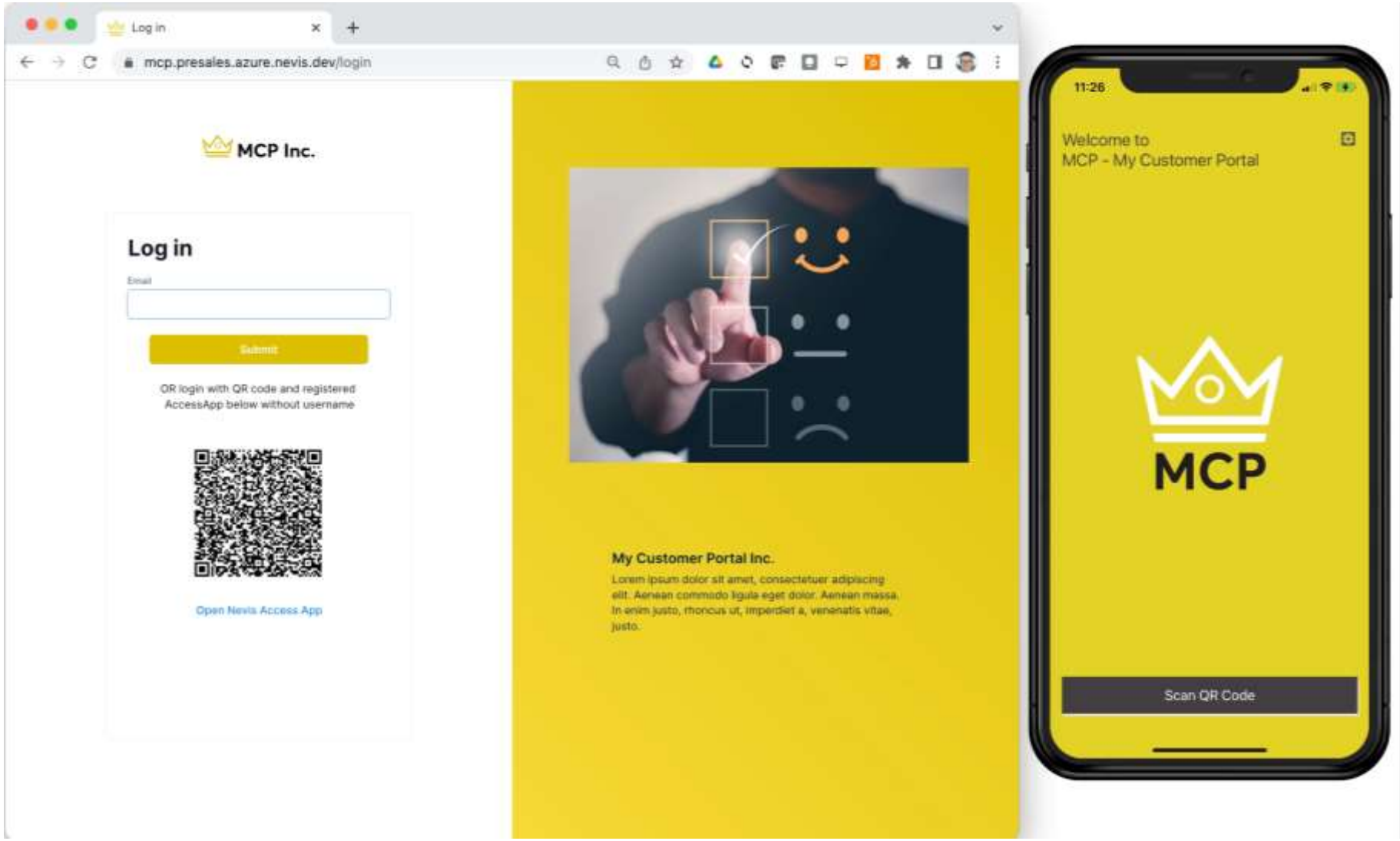
Resultate:

- User Consent für Onboarding Process
- Echtheitsprüfung des ID Dokuments (AI Model)
- Liveness Detection
- Abgleich lebende Person zu ID Dokument
- Verifizierte Attribute aus offiziellem Ausweisdokument

User Perspektive: Registration (FIDO UAF)



User Perspektive: Komfort Login (FIDO UAF)



Die Rolle der Biometrie in der passwortfreien Authentisierung

Wichtig: Biometrische Informationen verlassen das Gerät niemals

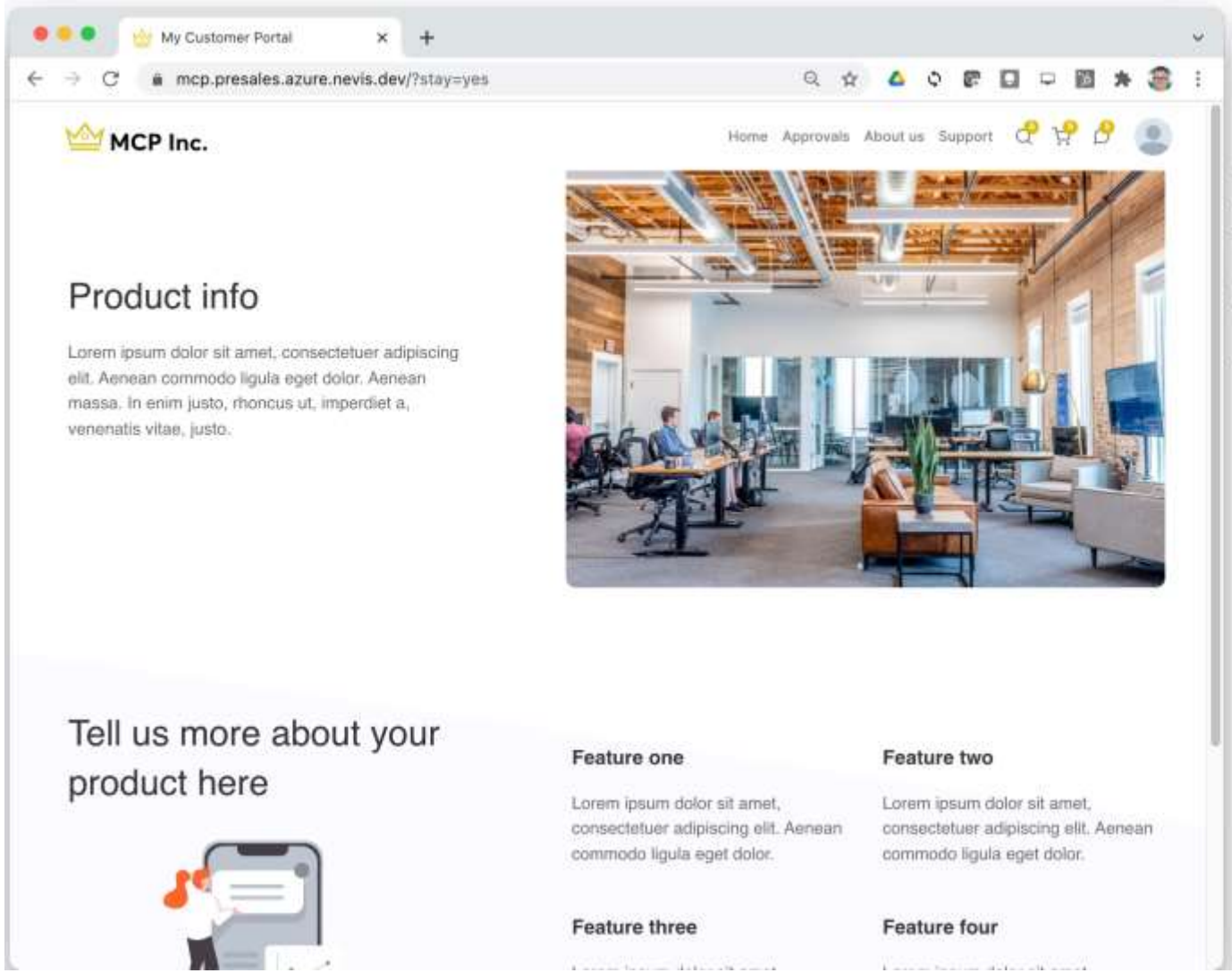
2-Faktor-Authentisierung:

- Smartphone-basiert
  (etwas, das ich besitze)
- Nutzt die biometrischen Möglichkeiten des Smartphones
  (etwas, das ich bin)
- Ziel: einfachere Bedienung und höhere Sicherheit als Passwörter

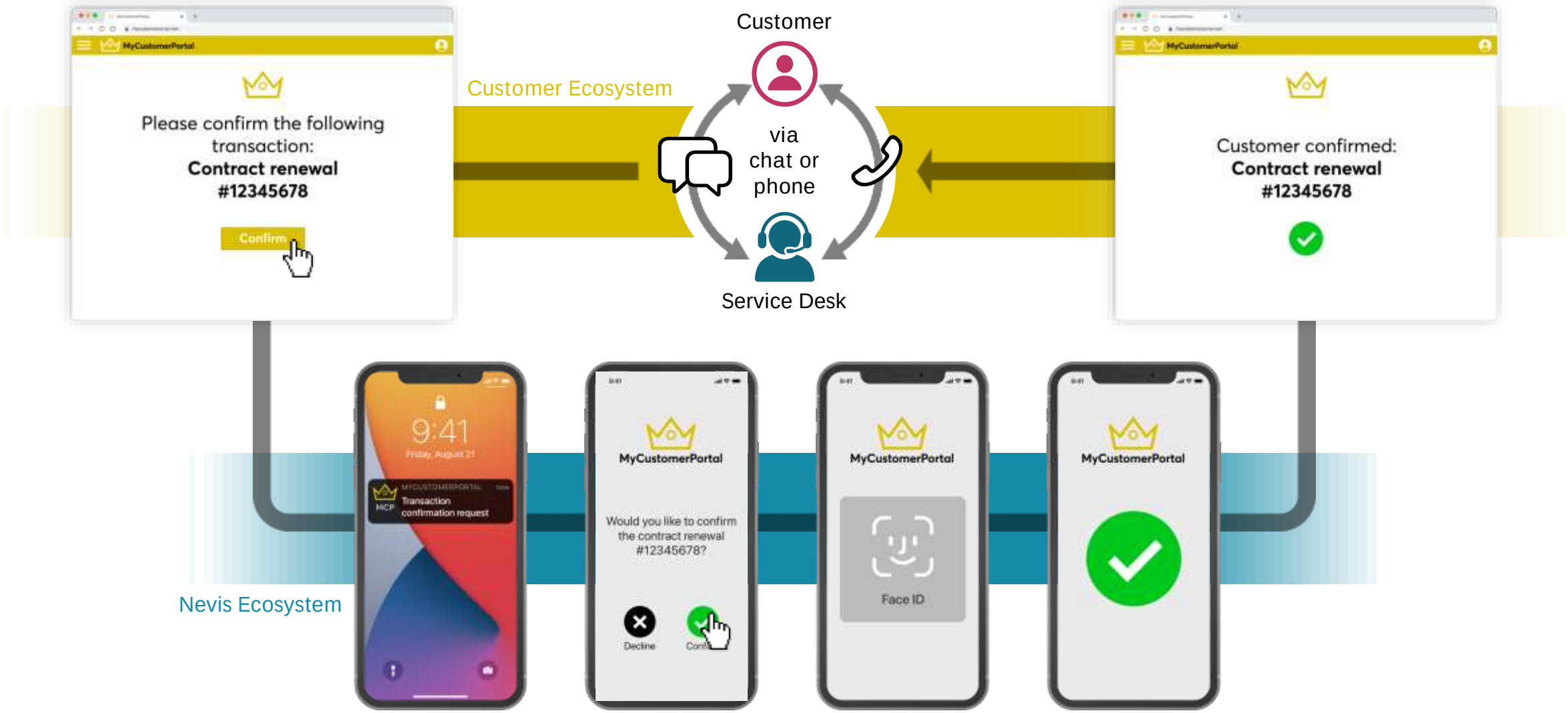
Über die Authentisierung hinaus

Transaktions-bestätigung

User Perspektive: **Transaktionsbestätigung**

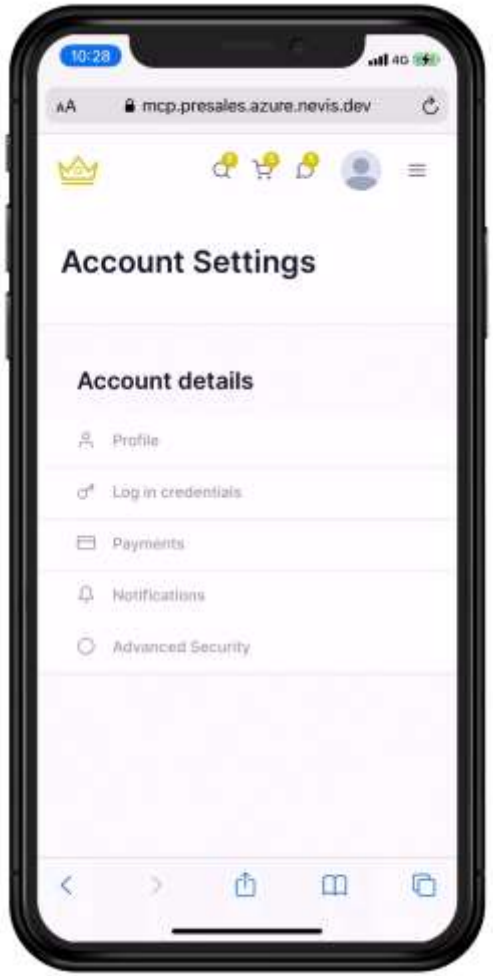


Service Desk Authentication/Authorization

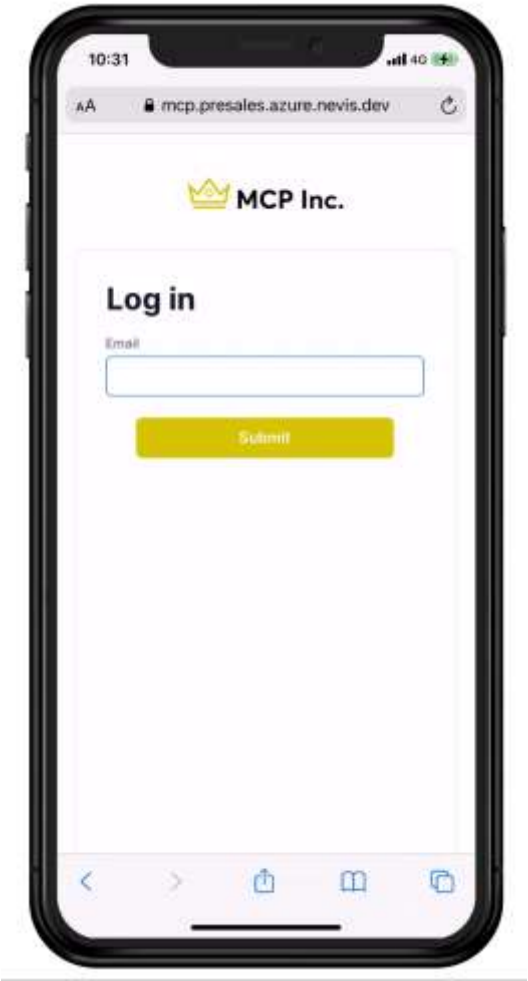


User Perspektive: Passwortfrei ohne App

User Perspektive: Mobile Registration (FIDO WebAuthN)



User Perspektive: Mobile Login (FIDO WebAuthN)



Security Architektur

Das grosse Bild: Ein ganzheitliches Konzept

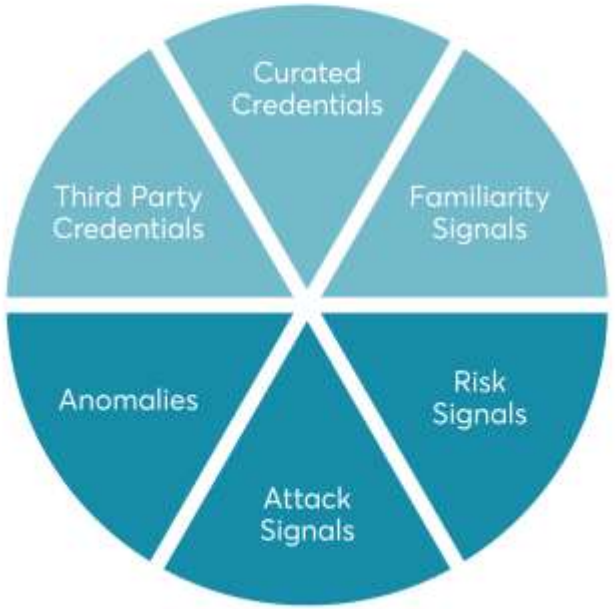
Schau mal, ganz ohne Passwort!

Eine reibungslose User Journey

Identity Trust Evaluation

Collect identity signals

Evaluate identity



nevisDetect

Mitigate (if necessary)

- Authorization step-up
- Notify user
- Notify support desk
- Lock Account

Nevis Mobile Authentication

fido CERTIFIED UAF

Nevis Deployment Optionen

Identity Suite

Identity Suite
Full-fledged CIAM for complex requirements

Flexible combination of use cases by configuration patterns

Many Applications
(typically heterogeneous)

Self-Managed,
Public- or private Cloud, On Prem

Authentication Cloud

Other Platform
Finance Portals, Gaming Platforms, Health Insurance Portals, etc.

Low-Code, standard Integrations

Authentication Cloud
- Passwordless Authentication
- ID Verification

Software as a Service (SaaS)

Identity Cloud

Identity Cloud
Fast deployment thanks to highly standardized use cases

No-Code, standard Integrations and Processes

Standard Applications
(including SaaS Services)

Software as a Service (SaaS)

Was unsere Kunden sagen

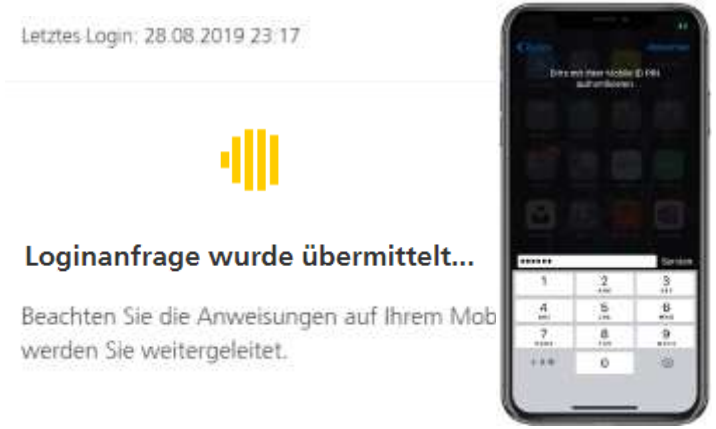
Ausgangslage «Einheitlicher Digitaler Zugang»

Login mit Kartenlesegerät

- Benutzername
  + Passwort
  + Eingabezahl + PIN
  + Code von Kartenleser

- Für Zugang E-Finance, Zahlungs-Authentisierung, Dienste-Aktivierung
- Benötigt Karte und **Kartenlesegerät**

Login mit Mobile ID



- Benutzername
  + Passwort
  + Mobile ID PIN

- Für Zugang E-Finance
- Benötigt Mobile ID-fähige SIM-Karte und aufwändigen Aktivierungsvorgang

Login mit Schnellservice

- Passwort oder Touch ID genügen

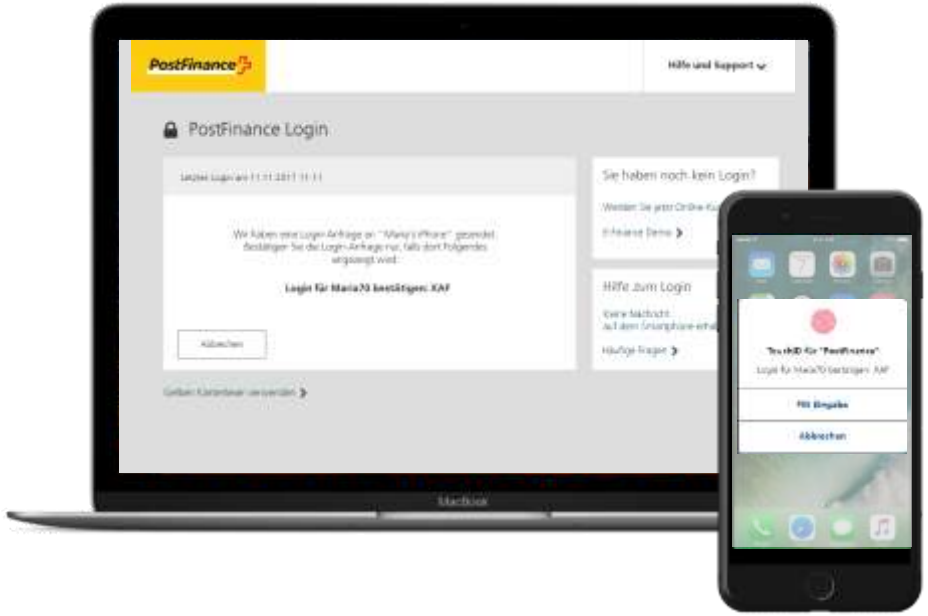
- Nur via App für **ausgewählte Funktionen,** kein «Step-Up» für vollen Zugriff
- Benötigt App und Anmeldung

Eingeschränkte Benutzerfreundlichkeit für uneingeschränkten E-Finance Zugang.
Schnellservice App mit gutem Benutzererlebnis.

Zielbild **«Einheitlicher Digitaler Zugang»**

In-App Login

Desktop Login



VERBESSERUNGEN

- Einfache Authentisierung: Nutzung biometrischer Verfahren
- Single Sign-On: Zugang zu allen Angeboten durch einmaliges Anmelden
- **Verfügbarkeit:** Bankgeschäfte jederzeit und überall möglich
- **Erhöhte Sicherheit:** Transaktionssignierung bei risikobehafteten Zahlungen

Maximale Benutzerfreundlichkeit für uneingeschränkten E-Banking-Zugang.

Was passwortfreies **Login für Sie** bewirken kann

- 2-**3 mal höhere Interaktionsrate** der Kunden bei passwortfreiem Login
- Nach 12 Monaten nutzen mehr als 1 Million User die passwortfreie Authentisierung
- Nach 12 Monaten sind mehr als zwei Drittel aller Logins passwortfrei
- Mobile first: 4 Mobile-App-Logins auf 1 Desktop-Login!
- Keine Kostensteigerung beim Callcenter-Support

„Unsere Kunden schätzen den passwortfreien und sicheren Zugang zu ihrem Konto: Die Zahl der Kundeninteraktionen hat sich verdoppelt.“

Eric Müller
Lead Solutions Architect, PostFinance

PostFinance

Was sagen unsere Kunden?

88% stufen das neue Login über die mobile App im Vergleich zu einem Kartenleser-Login als besser oder viel besser ein

82% stufen das neue Login im Vergleich zum Login mit Mobile ID* als besser oder viel besser ein

97% werden weiterhin das neue Login nutzen

93% werden das Login anderen Nutzern weiterempfehlen

*verschlüsselter, SMS-basierter Login-Mechanismus

„Unsere Kunden schätzen den passwortfreien und sicheren Zugang zu ihrem Konto: Die Zahl der Kundeninteraktionen hat sich verdoppelt.“

Eric Müller
Lead Solutions Architect, PostFinance

PostFinance

Schlussfolgerung

Zum ersten Mal: Verbesserte Sicherheit und Benutzererfahrung gehen Hand in Hand!

Die Vorteile

- Das Eliminieren von Passwörtern ist ein riesiger Sprung in der Verbesserung der End-to-End-Sicherheit
- Bessere Kundenerfahrung bewirkt mehr Interaktion, insbesondere über den mobilen Kanal
- **Niedrigere Kosten für Support**- und Helpdesk – kein Zurücksetzen von Passwörtern
- Transaktionsbestätigung eröffnet neue **Anwendungsmöglichkeiten**

Danke!

Bitte am Ausgang mitnehmen – mit Download-Link zur Studie - Stand 7-632

+41 43 215 29 09

Birmensdorferstrasse 94
8003 Zürich

info@nevis.net
holger.hinzmann@nevis.net

www.nevis.net