complex
GmbH & Co. KG

ZUKUNFT PASSWORD(LESS)

Kontextbezogene Sicherheitsstandards so aufbauen, dass Umsatzbremsen vermieden werden.

Ein Vortrag von Ulrich Monjau und Pascal Pischel

Wir sind keine Sicherheitsfirma – wir sind digitaler Branchenpartner

Seit vielen Jahren begleiten wir den Automobilhandel in seiner digitalen Transformation – **strategisch, technologisch und operativ**.

Wir ersetzen keine Systeme, sondern passen unsere Online Vertriebs und Service Module in bestehende Systemlandschaften ein. Wir nutzen dort vorhandene Strukturen und Informationen, sodass frühestmöglich schon Umsatz erzeugt werden kann.

Mit Partnern wie **Kunzmann** haben wir über Jahre hinweg erfolgreiche Projekte umgesetzt, die mehrfach ausgezeichnet wurden – unter anderem mit dem **Digital Dealer Performance Award (2020–2024)**, dem **Top Shop 2024** und dem **Automotive Business Award**.

Diese Erfolge zeigen**: Wir verstehen, wie Digitalisierung im Autohaus funktioniert, wirtschaftlich wirkt und nachhaltigen Mehrwert schafft.**

Auch bei frühstmöglicher Marktverfügbarkeit müssen wir für unsere Betreiber immer Performance und Sicherheit gewährleisten!

IT-PERFORMANCE & SICHERHEIT

Ein großer Themenbereich und nur 25 min...

Das Digitale-Service-Erlebnis als Hürdenlauf

IT-Performance & Infrastruktur

- Serveroptimierung – Maßnahmen zur Steigerung der Leistungsfähigkeit und Stabilität von Servern.
- Cloud-Skalierung – Dynamische Anpassung von Cloud-Ressourcen an aktuelle Lastanforderungen.
- Netzwerkarchitektur – Aufbau und Strukturierung eines effizienten, sicheren IT-Netzwerks.
- Latenzmanagement – Reduzierung von Verzögerungen bei Datenübertragung zur Verbesserung der Performance.
- Edge Computing – Verarbeitung von Daten nahe an der Quelle, um Reaktionszeiten und Bandbreite zu optimieren.

Systemüberwachung & Analyse

- **Monitoring Tools** – Softwarelösungen zur Überwachung von Systemzuständen, Performance und Verfügbarkeit.
- **Incident Response** – Vorgehensweise zur schnellen Reaktion und Behebung von Sicherheitsvorfällen.
- **Log-Analyse** – Auswertung von System- und Anwendungsprotokollen zur Fehler- und Sicherheitsanalyse.
- **Anomalieerkennung** – Automatisches Erkennen ungewöhnlicher Muster im Systemverhalten.
- **Predictive Maintenance** – Vorausschauende Wartung auf Basis von Analysedaten, um Ausfälle zu vermeiden.

IT-Sicherheit & Schutzmaßnahmen

- **Zero Trust** – Sicherheitsansatz, der keinem Nutzer oder Gerät standardmäßig vertraut und jede Anfrage prüft.
- **Identitätsmanagement** – Verwaltung digitaler Identitäten zur Kontrolle von Zugriffsrechten und Authentifizierungen.
- **Single Sign-On (SSO)** – Einmalige Anmeldung ermöglicht sicheren Zugriff auf mehrere Systeme ohne erneutes Login.
- **Penetration Testing** – Simulierte Angriffe zur Identifikation und Behebung von Sicherheitslücken.
- **Threat Intelligence** – Sammlung und Analyse von Bedrohungsdaten zur frühzeitigen Erkennung von Angriffen.
- **Datenverschlüsselung** – Schutz sensibler Informationen durch codierte Speicherung und Übertragung.

Organisation & Prozesse

- **DevSecOps Integration** – Einbettung von Sicherheitsaspekten in Entwicklungs- und Betriebsprozesse.
- **IT-Governance** – Regelwerke und Prozesse für verantwortungsvolle, sichere IT-Steuerung.
- **Compliance Management** – Sicherstellung der Einhaltung gesetzlicher und regulatorischer Anforderungen.
- **Risikoanalyse** – Systematische Bewertung von IT-Risiken zur Risikominderung.
- **Business Continuity** – Strategien zur Aufrechterhaltung des Geschäftsbetriebs bei IT-Störungen.

Zukunft & Innovation

- **KI in Security** – Einsatz künstlicher Intelligenz zur Erkennung und Abwehr von Cyberbedrohungen.
- **Quantum Security** – Schutzmechanismen gegen Angriffe durch Quantencomputer.
- **Autonomous Systems** – Selbststeuernde Systeme mit eigenständigen Sicherheitsmechanismen.
- **Secure Cloud Native** – Sicherheitskonzepte speziell für Cloud-Native-Anwendungen.
- **Sustainable IT** – Nachhaltige IT-Lösungen, die Energieeffizienz und Umweltaspekte berücksichtigen.

Wenn man lange genug in einem Unternehmen ist, erkennt man zwei Lager, die das Unternehmen entwickeln wollen
> aber auf sehr unterschiedliche Weise.

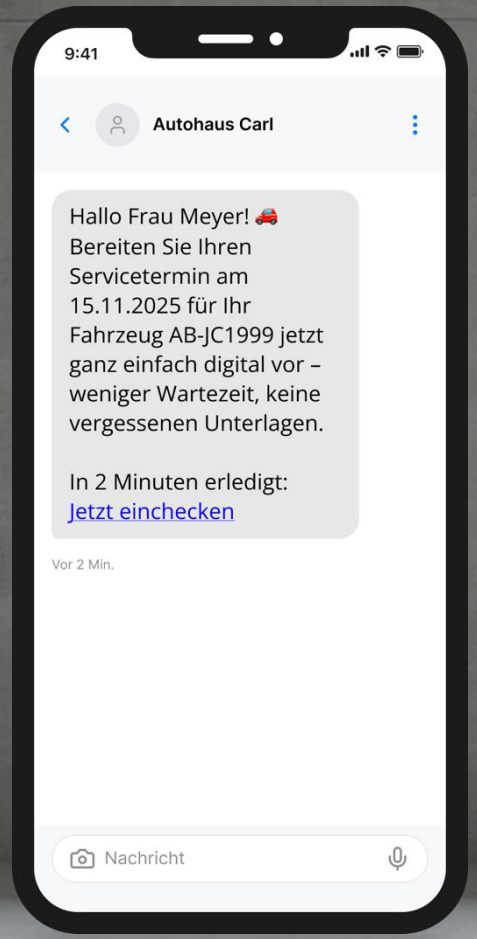
Die IT schützt uns vor Risiken. Der Onlinevertrieb schützt uns vor Umsatzverlust.

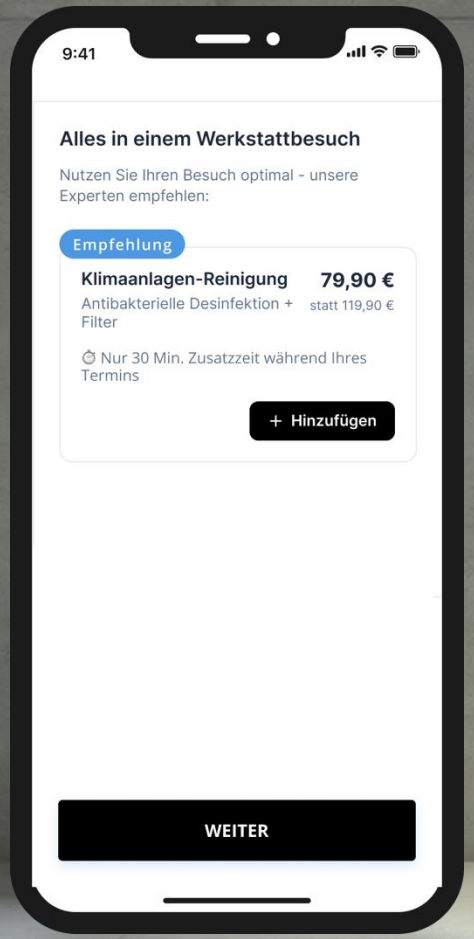
Und manchmal hat man das Gefühl:
„Der Kunde steht genau dazwischen – mit drei Login-Fenstern und schwindender Geduld."

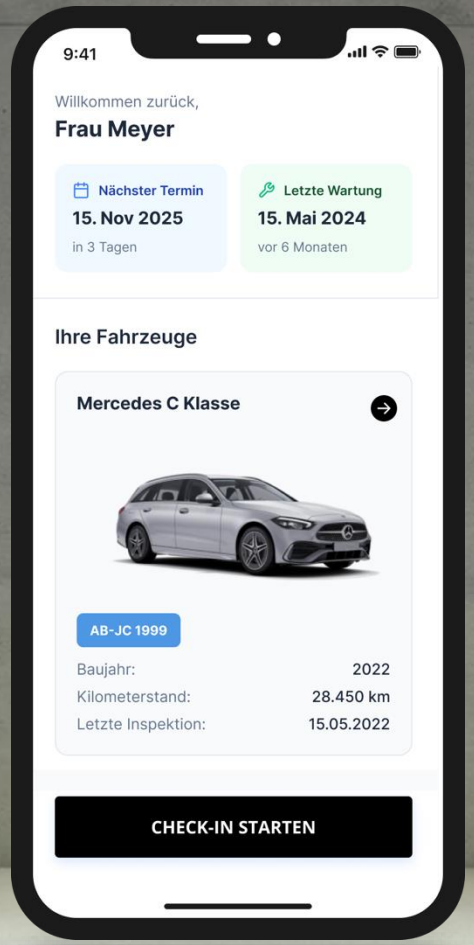
Beide Seiten haben Recht!
Nur: Sicherheit kostet. Und zwar nicht nur Geld, sondern auch Conversion, Vertrauen und Zeit.

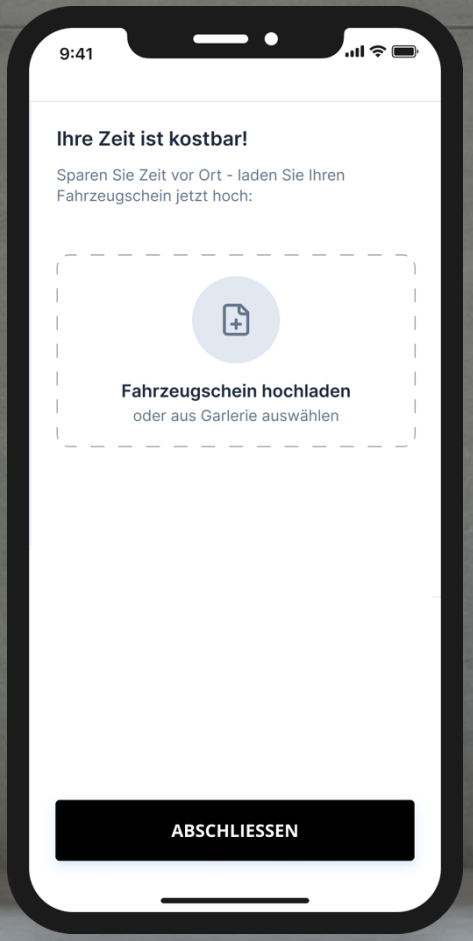
Wenn wir also über Performance reden, reden wir nicht nur über Rechenleistung, sondern über Geschäftstempo.

Digitaler Service in Ihrem Autohaus

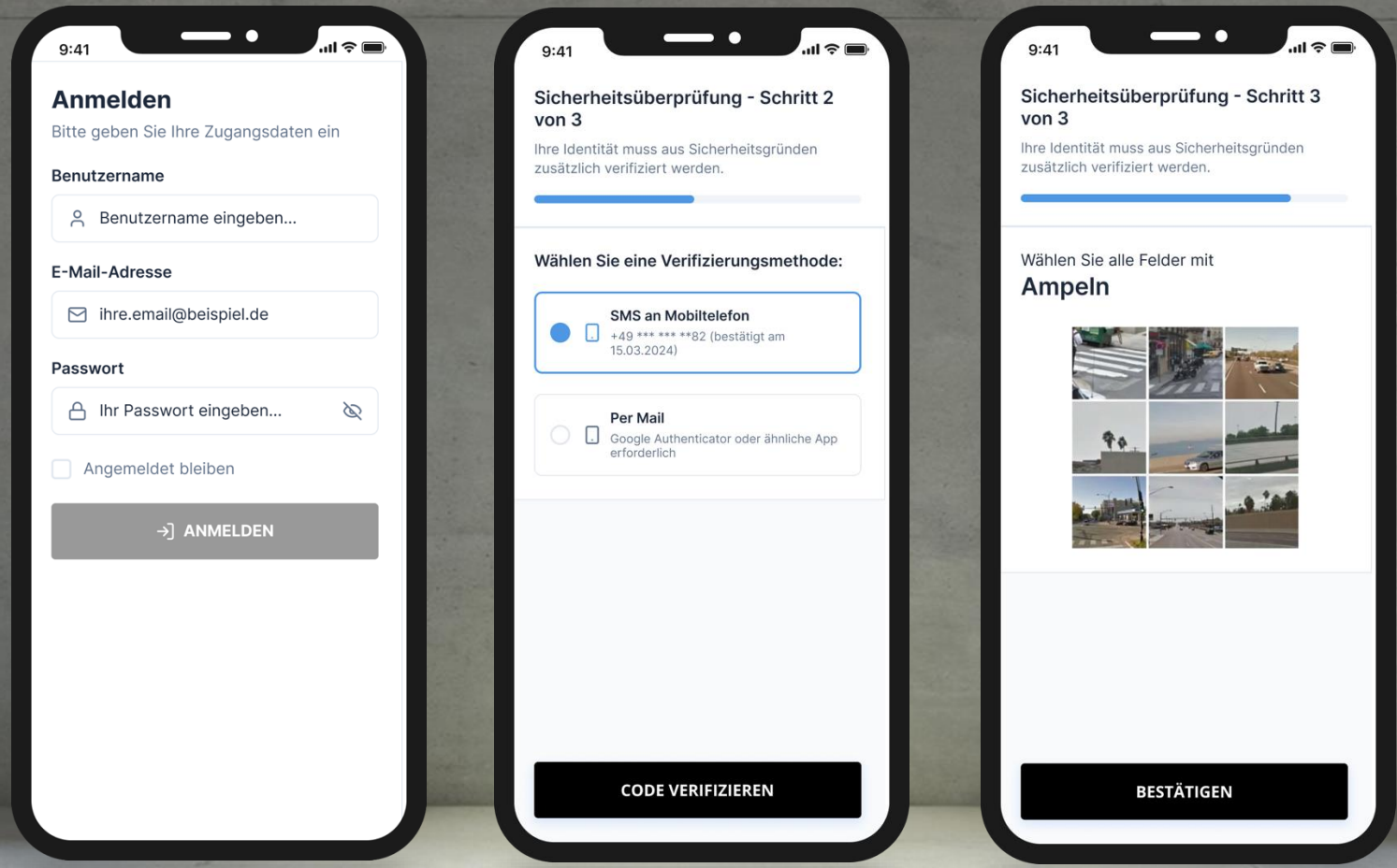




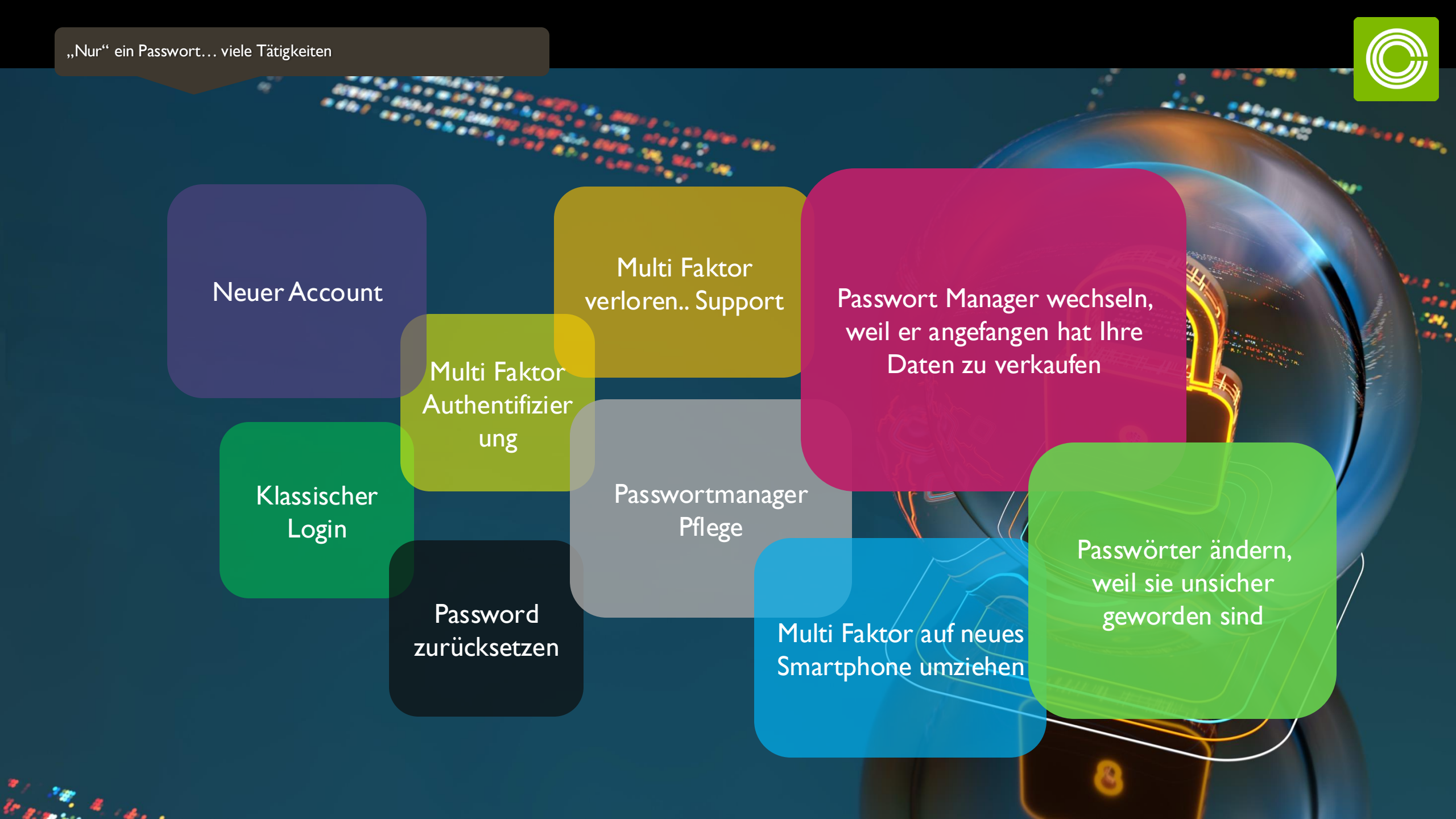




Führerschein und Fahrzeugpapiere bitte...



„Nur“ ein Passwort… viele Tätigkeiten



45-60 Tage

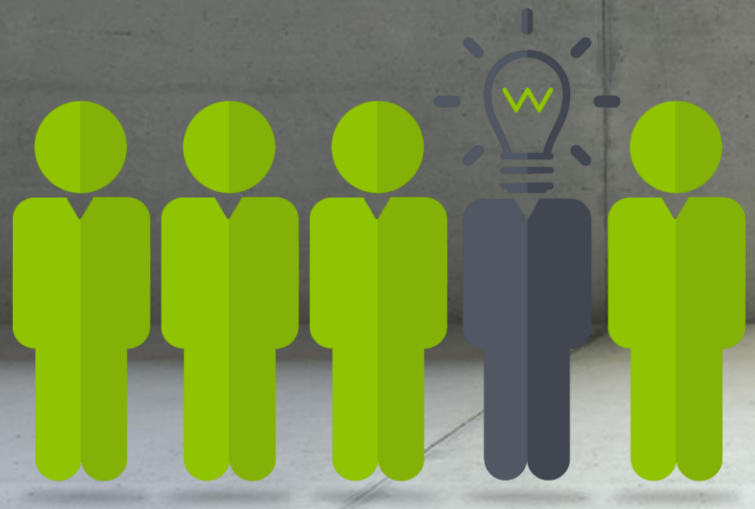
Verbringen auch Ihre potenziellen Kunden mit Passwörtern

und User-Logins im Leben

Sehr lang haben Nutzer von Anwendungen das akzeptiert.

Das Bewusstsein für unnötige Aufwände wird größer und damit auch eine klare Haltung bei zu hohen „Rüstungsaufwänden“ zur Nutzung digitaler Anwendungen.

Mit viel Mühe bringen nicht nur Autohäuser Ihre Kunden in digitale Strecken. 24/7 Verfügbarkeit und zentrale Qualitätststeuerung sollen Mehrumsatz und Kundenbindung erzeugen und dann stoßen wir sie wieder in den Anruf beim Servicecenter, weil wir die Eingangstür „verrammeln“.



- Ergonomie, Benutzererfahrung und Komfort entscheiden heute aufgrund der hohen Verfügbarkeit darüber, ob Nutzer kaufen oder gehen…

Komfort trifft Sicherheit!
Digitale Services stehen heute zwischen zwei Erwartungen:

Sicherheit für das Unternehmen und **Komfort für die Nutzer**.

Passwörter allein werden nicht mehr als sicher angesehen. Zwischen gar keiner Zugangsprüfung und Single Sign-On befindet sich ein weites Feld. Single Sign-On (SSO) und damit PASSWORDLESS wird oft als Ideal beschrieben– doch er funktioniert nicht für jede Zielgruppe gleich gut.

Sicherheit ist kein Einheitsprodukt – sie muss so differenziert sein wie das, was wir schützen.

Ob Schokolade oder Kreditkarte – das Maß an Sicherheit sollte immer zum Risiko passen.

Was möchte ich sichern?

Wer bekommt welche Schlüssel?

Wer geht denn durch diese Tür?

Wie oft möchte ich durch diese Tür gehen?

1 Fall 1: Terminbestätigung – der harmlose Token

Ein Kunde bekommt eine E-Mail:
„Ihr Servicetermin am 12. November – bitte bestätigen Sie mit einem Klick."

Das ist ein klassischer Token-Login.

Der Klick bestätigt nur: „Ja, ich komme."

Keine Daten werden geändert, keine Verpflichtung eingegangen.

Falls jemand Fremdes den Link anklickt, ruft das Autohaus vielleicht an und fragt:
„Haben Sie Ihren Termin vergessen?"

Mehr passiert nicht – genau wie im echten Leben.
Technisch: Der Token ist einmalig, zeitlich begrenzt und ohne Passwort.

Perfekt für harmlose, schnelle Interaktionen.

2

Fall 2:
Im gebuchten Termin zusätzlichen Service buchen – der einfache Zugang mit Mini-Check

Hier soll der Kunde im Rahmen eines bestehenden Termins eine Zusatzleistung dazubuchen– z. B. eine Klimaanlagenreinigung.

Er klickt den Token-Link in der E-Mail, landet direkt im Terminportal, bucht den Service mit 1 Click und bestätigt am Ende mit seiner Postleitzahl.

Einfach, direkt, ohne großes Login.

Die Hürde ist niedrig – aber es gibt eine kleine Sicherheitsprüfung am Schluss.

Denn die Postleitzahl weiß fast jeder, aber sie verhindert, dass ein völlig Fremder einfach etwas ändert. Optional noch eine Mail an den Auftraggeber die das der Ordnung halber nochmal bestätigt.

Technisch: Ein tokenbasierter Zugang mit leichter Verifikation, ideal für Vorgänge, die schnell gehen sollen, aber nicht völlig offen sein dürfen.

3

Fall 2:
Fahrzeugdaten ändern oder Service buchen > jetzt wird es ernst!

Nun geht es um sensible Daten oder verbindliche Aktionen wie z. B. Fahrzeugschein ändern, neues Auto anmelden oder digitale Fahrzeugschätzung durchführen.

Hier reicht ein einfacher Token-Link nicht mehr aus. Der Nutzer muss sich über ein Login anmelden – also mit Benutzername, Passwort und ggf. zweitem Faktor. Oder eben SSO bspw. über Apple.

Nur so ist sichergestellt, dass wirklich die richtige Person Zugriff bekommt.

Technisch: Das Single Sign-On nutzt eine dauerhaft geprüfte Identität.

So lässt sich nachvollziehen, wer was wann getan hat – wichtig für Sicherheit und Datenschutz.

Eine bequeme Variante, die hohen Schutz bietet, ohne ständig „Passwort vergessen“ durchzuspielen.

Viele Marken und Systeme aber trotzdem „one face to the Customer“ mit einem übergreifenden Sicherheitskonzept und dem richtigen Verfahren für den richtigen Zweck!

1

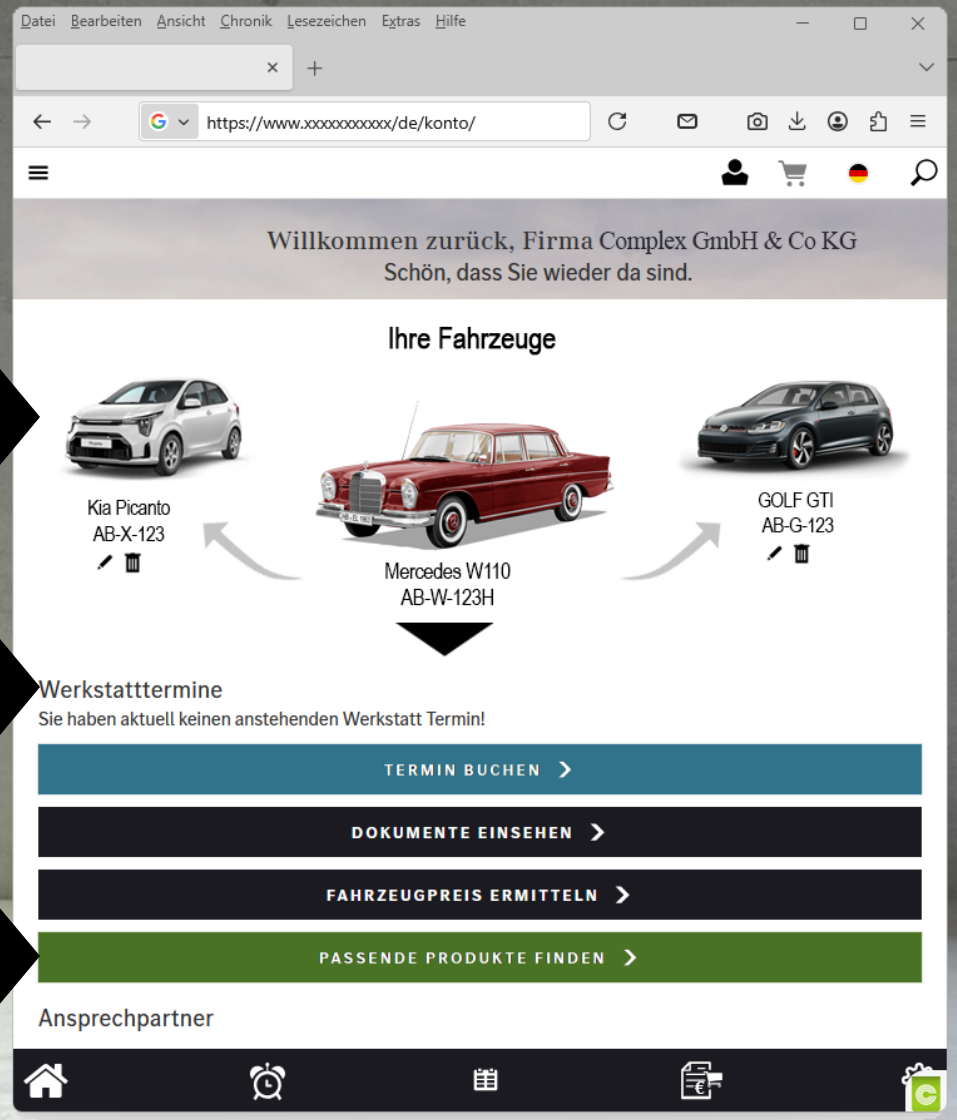
Tokenlogin
Schnell, bequem, niedrig-schwellig, für einfache oder harmlose Aktionen.

2

Token + Mini-Check
Praktisch für seltene, aber persönliche Vorgänge z. B. Terminbuchung.

3

Single Sign-On (SSO)
Pflicht, sobald Daten verändert oder Zahlungen ausgelöst werden.



Zugänge sind Wirtschaftsfaktoren

Sicherheit **genau dort und in der Qualität**, wo und wie sie gebraucht wird.

Ökonomische Lenkung statt technischer Abschottung

„Wenn unsere Kunden mehr **Zeit** beim Anmelden als beim Nutzen verbringen, haben wir **kein** Sicherheitsproblem, sondern ein Geschäftsproblem.“

DANKE FÜR IHRE AUFMERKSAMKEIT!

Ein Vortrag von
Ulrich Monjau und Pascal Pischel
www.complex-it.de