RSA

Clear Skies: Was passiert, wenn es keine Cloud mehr gibt?

Erik Teschner
Systems Engineer, RSA

16.09.2025, Congress Park Hanau

CLEAR SKIES: WAS PASSIERT, WENN ES KEINE CLOUD MEHR GIBT?

Erik Teschner

Systems Engineer

erik.teschner@rsa.com

DIE ERHOLUNG NACH EINEM AUSFALL IST GAR NICHT SO LEICHT

Das Ziel der **Disaster Recovery** besteht darin, im Falle eines Ausfalls das das Unternehmen **am laufen zu halten.**

Die Recovery von einem Disaster kann bedeuten, dass folgende Dinge **eingeschränkt** sind:

- Funktionalität
- Benutzerfreundlichkeit
- Performance

The lights might be dimmed… but there will be light!

CLOUD-BASIERT

Identity & Access Management und insbesondere MFA werden zunehmend über die **Cloud** bereitgestellt.

Der sichere Betrieb einer IAM-Infrastruktur ist nicht einfach, SaaS-Anbieter können dies **in vielen Fällen besser.** Übliche Vorteile von SaaS, z. B.

- **einfache Updates**
- **geringere Betriebskosten**
- **Neue Funktionen** tauchen einfach eines Tages auf

DARUM IST NIS2 WICHTIG!

Ein verpatztes Update von **Crowdstrike** am 19. Juli 2024 führte zu weitreichenden kompletten Systemausfällen.

Großer Ausfall **mehrerer Systeme** und Anwendungen.

Dies könnte viele andere Gründe mit mehr oder weniger weitreichenden Auswirkungen haben, wie z.B. **DDoS**, **Naturkatastrophe** o.ä.

5

ALSO, WAS IST IHR PLAN?

In der Luftfahrt werden bei Problemen mit dem Flugzeug **Checklisten** verwendet. Piloten werden darauf trainiert, sich auf die dringendsten Probleme zu konzentrieren: **Fliegen, Navigieren, Kommunizieren.**

Für IT-Systeme: Halten Sie einen **Plan**, Verfahren und Technologien bereit, die Ihnen dabei helfen, sich nach einem Ausfall sicher zu erholen:

- **Rechnen Sie damit, dass Dinge schiefgehen werden**.

- Halten Sie diesen **Plan** verfügbar und auf dem neuesten Stand.

- Schulen Sie die Mitarbeiter darin, den Plan zu befolgen.

- Halten Sie die richtige **Architektur** und **Technologie** bereit.

- Konzentrieren Sie sich darauf, die wichtigsten Anlagen wieder zum Laufen zu bringen.

6

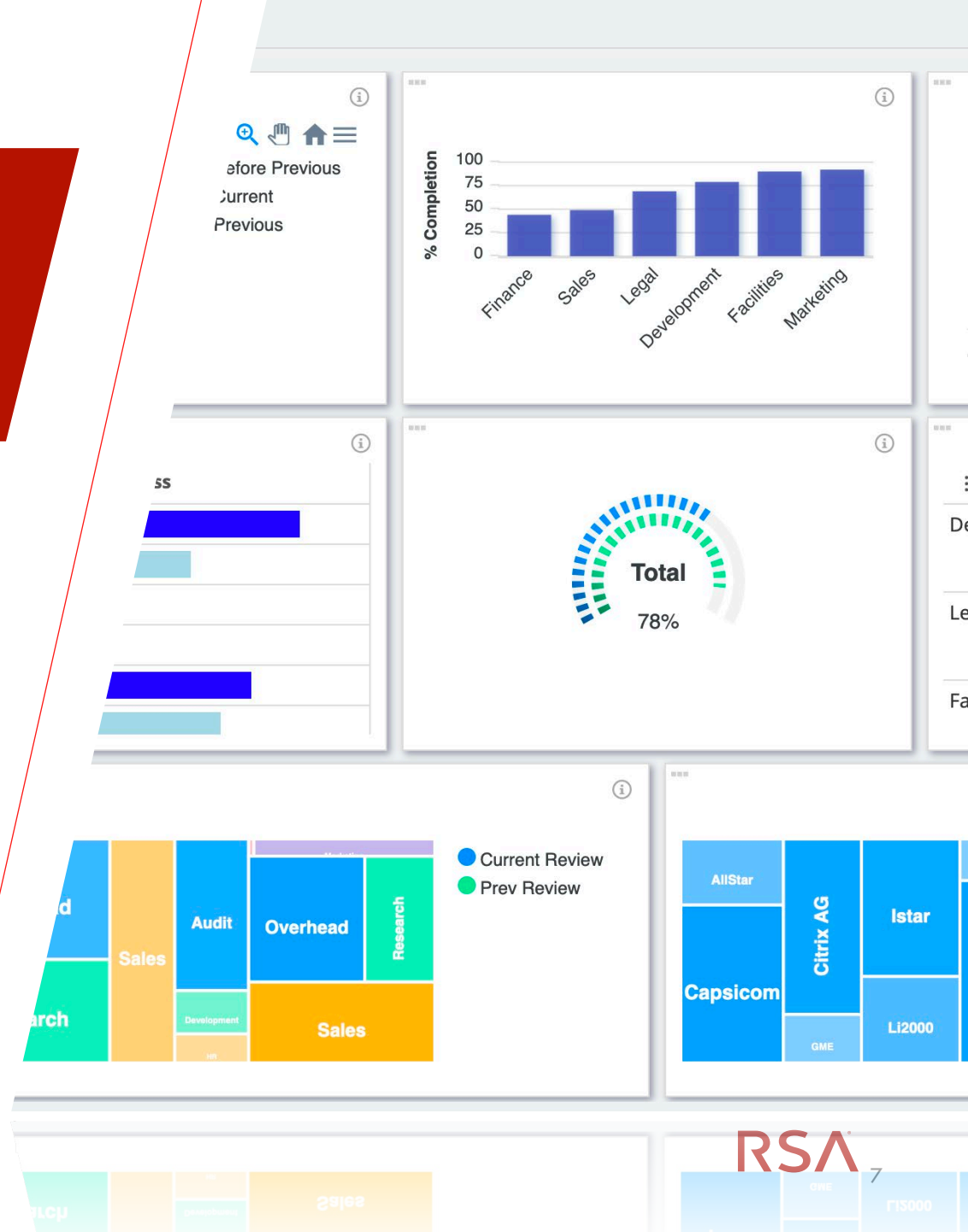
WAS WENN IGA-SYSTEME NICHT MEHR VERFÜGBAR SIND?

Keine aktuelle Übersicht über Identitäten, Zugriffe und Berechtigungen

Zugriffsüberprüfungen und -berichte nicht mehr verfügbar

Zugriffsanfragen/-genehmigungen und -erfüllung sind nicht mehr möglich

Account Takeover, SoD, verwaiste Konten etc. kann nicht mehr getrackt werden



MFA IST DOWN! WAS NUN?

Die Nichtverfügbarkeit von Cloud-basierter MFA kann viele Ursachen haben:

- Ausfall des zugrunde liegenden **Cloud-Anbieters**
- **Verbindung zur Cloud** ist unterbrochen
- Schwere Vertrauensprobleme aufgrund der **Kompromittierung des MFA-Anbieters…**
- „Echter“ **Ausfall der MFA-Lösung**

Potenziell sind alle Anwendungen (vor Ort oder in der Cloud) plötzlich nicht mehr zugänglich

- Email
- VPN
- CRM

9

ES GEHT NICHT NUR UM VERFÜGBARKEIT

CLOUD-IAM-AUSFALL DARF NICHT ZU **VERRINGERTER SICHERHEIT** FÜHREN

ANGREIFER KÖNNTEN DEN (MFA-)AUSFALL ÜBERHAUPT ERST **VERURSACHT** HABEN.

DIE CLOUD IST PERFEKT, BIS SIE ES NICHT MEHR IST

Ihr Plan für einen MFA-Ausfall sollte nicht lauten: - „Es ist Cloud-basiert, also können wir **nichts tun, bis es wieder online ist.“**

MFA-Funktionen On-Prem sind entscheidend, um

- den Betrieb aufrechtzuerhalten
- sicher **wiederherzustellen**

Die Einrichtung und Wartung eines **separaten MFA-Systems ist nicht kosteneffizient,** in vielen Fällen nicht möglich und verringert die Sicherheit.

11

BESSER: HYBRID!

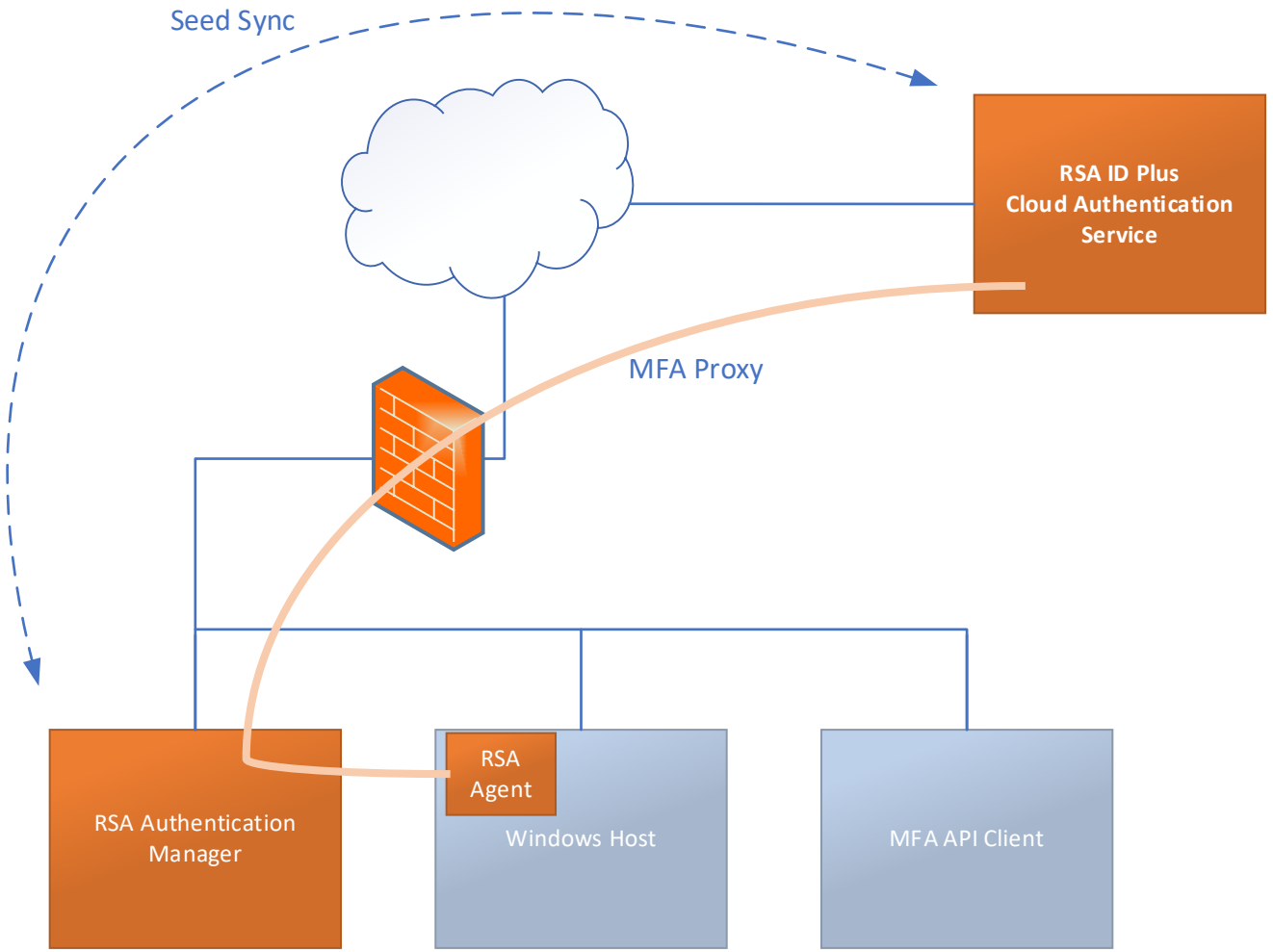
Eine echte hybride MFA-Bereitstellung stellt sicher, dass viele Anwendungen – insbesondere die **On-Premise-Anwendungen** – weiterhin durch MFA geschützt sind. Wenn die MFA-Cloud nicht mehr verfügbar ist, funktioniert der On-Premise-Teil weiter.

Sie müssen sich nicht mit den Problemen herumschlagen, die mehrere, unterschiedliche´

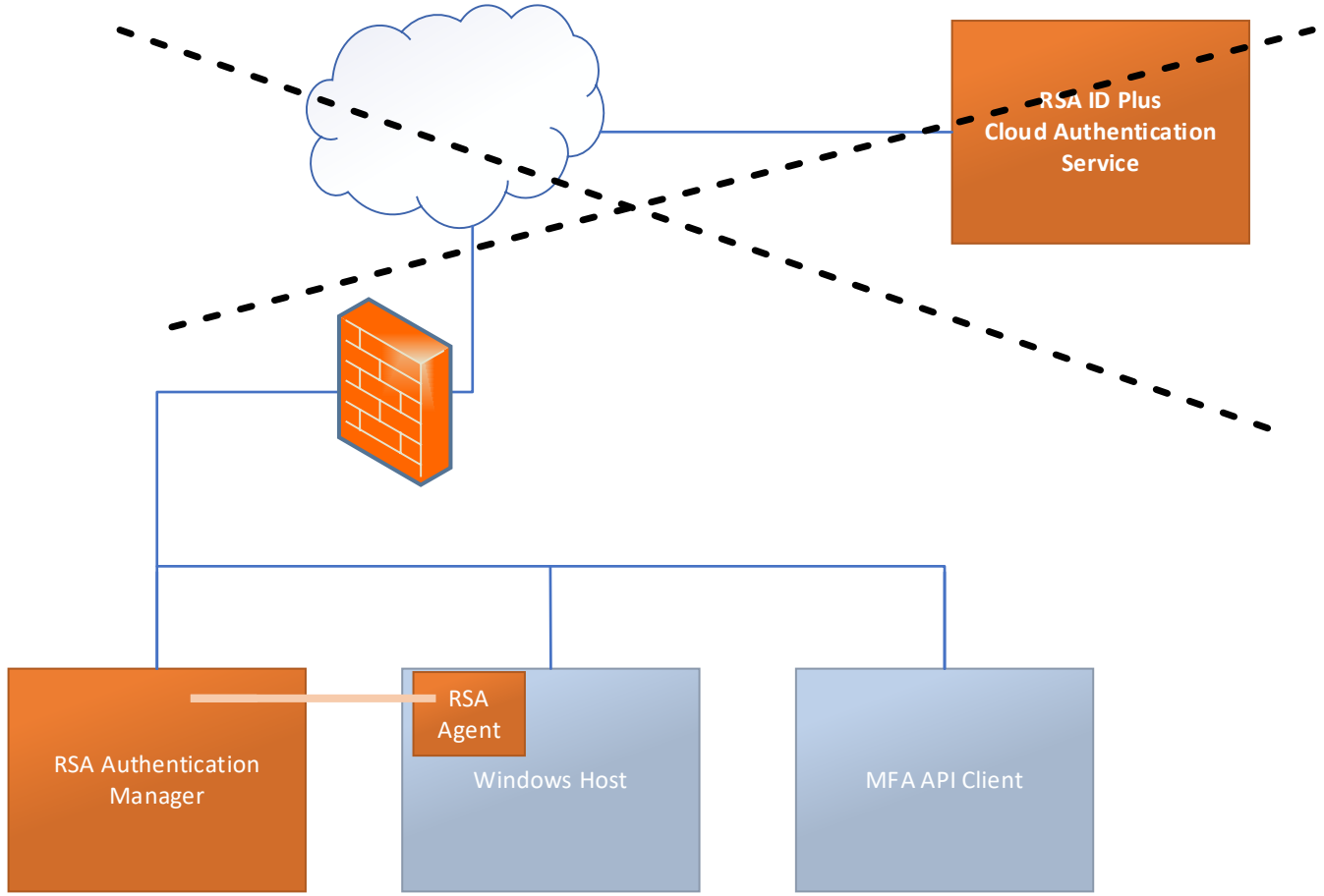
- **Authentifikatoren**
- **Lebenszyklusverwaltung inkl. Registrierungsabläufe**
- **Zugriffsrichtlinien** mit sich bringen.

12

RSA ID Plus Hybrid Deployment



Das ist schlimm … aber keine Katastrophe



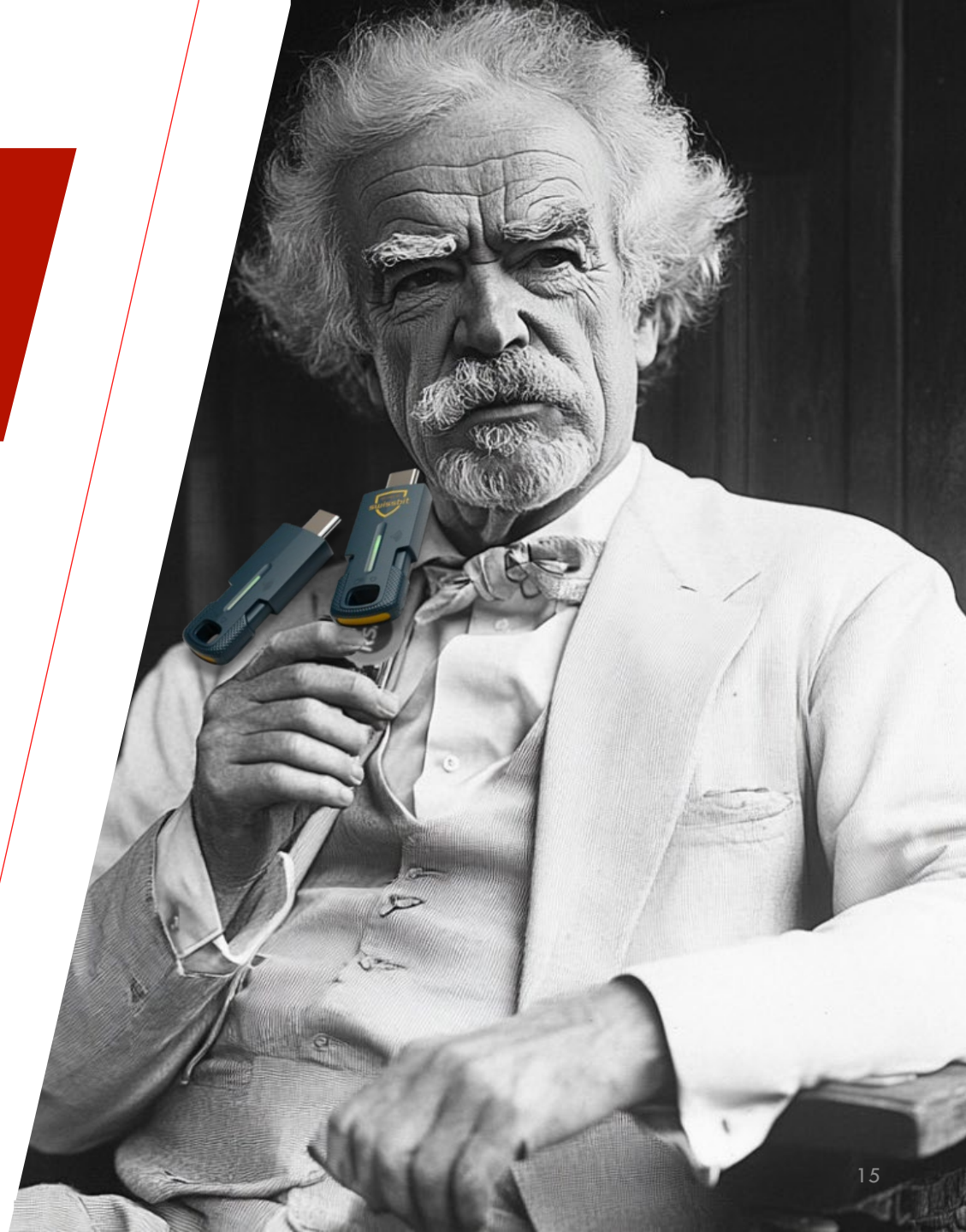
WAS WENN DIE CLOUD AUSFÄLLT?

Benutzer können kein FIDO mehr verwenden!

Es ist das gute alte **OTP**!

Der Tod von OTPs wird stark übertrieben.

Die Registrierung neuer Benutzer/Authentifizierer erfolgt bei Bedarf über den **RSA Authentication Manager.**



15

… ABER WARTEN SIE, ES GIBT NOCH MEHR!

Darüber hinaus sind echte **Offline-Modi** für die RSA-Agenten für **MS Windows und Apple macOS** verfügbar.

Benutzer müssen sich dann, ohne Verbindung zu einem MFA-Dienst, per OTP beim Betriebssystem anmelden.

-> Nicht nur Passwörter!

Offensichtlich erforderlich für Notebooks, die manchmal offline sind.

Nicht so offensichtlich, aber nützlich für z. B. **kritische Workstations und Server**, die zugänglich und sicher bleiben müssen.

16

- Fragen Sie sich vorab: "Was passiert, wenn unsere IAM/MFA-Cloud ausfällt?"
- Bereiten Sie sich auf dieses Szenario vor.
- RSA verfügt über das Know-how und die Technologie, um Sie zu unterstützen.

OWN YOUR IDENTITY.

RSA®

Controlware
Security Day

Danke für Ihre Aufmerksamkeit.
Wir freuen uns über Ihr Feedback!

Bitte geben Sie den ausgefüllten Bogen am Empfang ab und erhalten Sie als Dankeschön ein kleines Präsent.