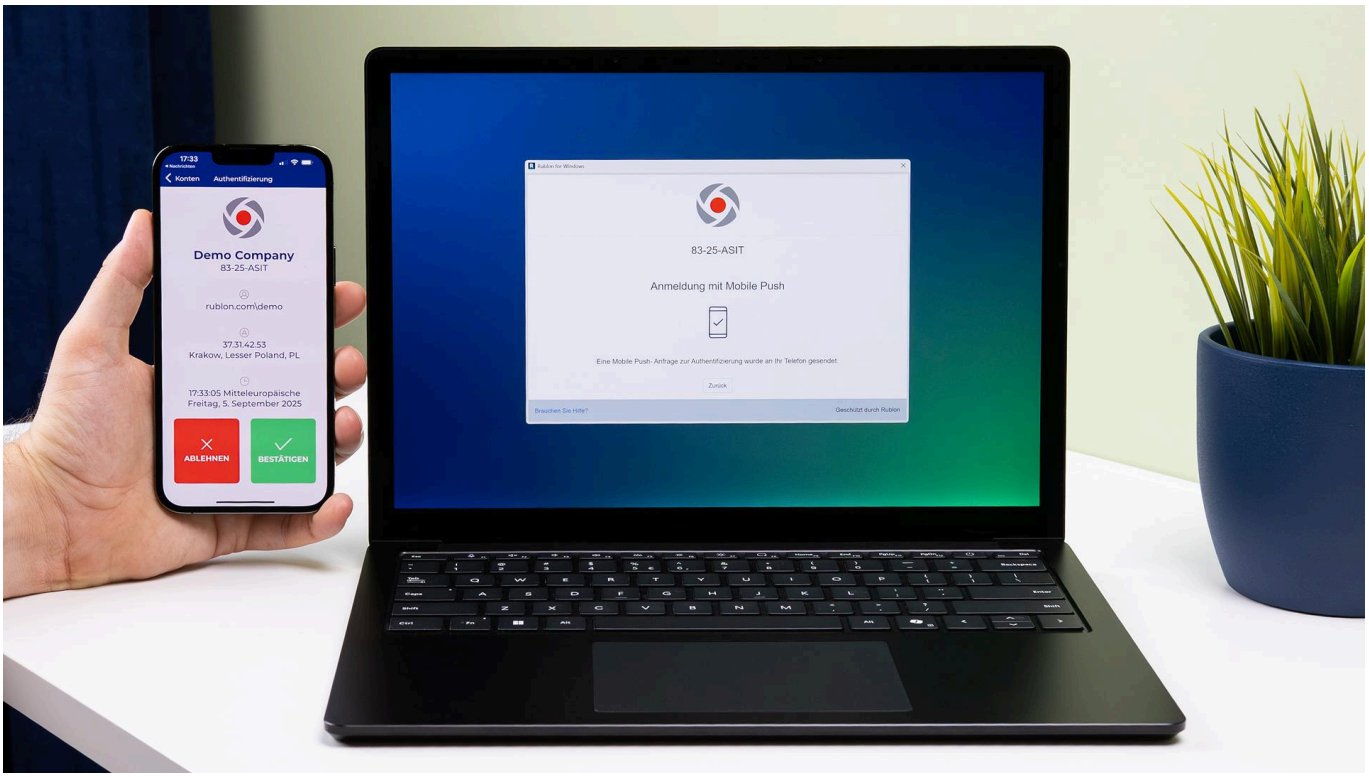
Rublon

# Leitfaden zur Implementierung der Multi-Faktor-Authentifizierung (MFA)

**Rublon sp. z o.o.**
ul. Stanislawa Wyspianskiego 11
65-036 Zielona Gora
Polen

www.rublon.de


17:33
Konten
Authentifizierung
Demo Company
83-25-ASIT
rublon.com\demo
37.31.42.53
Krakow, Lesser Poland, PL
17:33:05 Mitteleuropäische
Freitag, 5. September 2025
ABLEHNEN
BESTÄTIGEN
83-25-ASIT
Anmeldung mit Mobile Push
Eine Mobile Push- Anfrage zur Authentifizierung wurde an Ihr Telefon gesendet.
Zurück
Brauchen Sie Hilfe?
Geschützt durch Rublon

# Inhaltsverzeichnis

# 1. Einführung

Dieses Dokument ist ein umfassender Leitfaden zur Implementierung von MFA. Er richtet sich an Administratoren und IT-Spezialisten in öffentlichen Verwaltungen, im privaten Sektor sowie in anderen Organisationen, die dem nationalen Cybersicherheitssystem unterliegen.

Im Leitfaden finden Sie Antworten auf zentrale Fragen, die mit der Planung und Umsetzung der MFA-Implementierung verbunden sind:

- Wie wählt man einen geeigneten MFA-Anbieter aus?
- Wie bereitet man die Organisation auf die Implementierung vor?
- Wie führt man den Implementierungsprozess durch?
- Wie stellt man die kontinuierliche Funktionsfähigkeit der MFA-Lösung sicher?

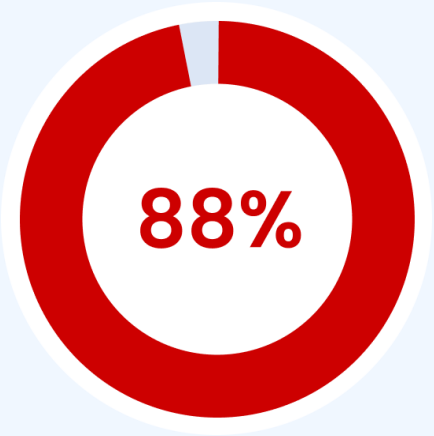
Der Leitfaden enthält außerdem einen Vergleich der Einsatzmöglichkeiten von MFA im Verbraucher- und Unternehmensumfeld sowie einen Überblick über die Sicherheitsaspekte verschiedener Authentifizierungsmethoden. Zusätzlich werden ein beispielhafter Implementierungsplan, praktische Checklisten für verschiedene Projektphasen sowie Diagramme und Tabellen mit den wichtigsten Informationen vorgestellt.

# 2. Was ist MFA?

Die Multi-Faktor-Authentifizierung (engl. multi-factor authentication, MFA) basiert auf der Verwendung von mindestens zwei voneinander unabhängigen Methoden zur Bestätigung der Identität eines Benutzers während der Anmeldung. Typischerweise bedeutet dies eine Kombination aus etwas, das der Benutzer **weiß** (zum Beispiel Passwort oder PIN), etwas, das der Benutzer **besitzt** (zum Beispiel ein Smartphone mit einer MFA-App oder einen Hardware-Schlüssel), und etwas, das der Benutzer **ist** (zum Beispiel ein Fingerabdruck oder ein anderes biometrisches Merkmal). Dank dessen erhält ein Angreifer selbst dann keinen Zugriff auf das Konto, wenn ein Authentifizierungsfaktor (z. B. ein Passwort) gestohlen oder kompromittiert wurde, da der zweite Faktor weiterhin erforderlich ist. In der Praxis erhöht MFA das

Sicherheitsniveau beim Zugriff auf Systeme und Daten erheblich, weshalb es sich lohnt, diese Form der Identitätsüberprüfung beim Anmeldevorgang zu aktivieren.

**Mehr darüber, was Multi-Faktor-Authentifizierung (MFA) ist, wie sie funktioniert und warum es sich lohnt, sie einzuführen, erfahren Sie in unserem Artikel: What is multi-factor authentication (MFA)?**




### Warum ist MFA wichtig?

Der Raport Verizon DBIR 2025 gibt an, dass etwa 88 % der Angriffe auf Webanwendungen auf der Verwendung gestohlener Passwörter basieren. Durch den Einsatz von MFA können Sie eine zusätzliche Sicherheitsebene hinzufügen, die bis zu 99 % der Angriffe auf Kontenübernahmen verhindern kann, selbst wenn die Angreifer das Passwort kennen.

Ein spezieller MFA-Typ, der als „Phishing-resistente MFA“ bezeichnet wird, erschwert außerdem Phishing-Angriffe, bei denen ein Opfer sein Passwort unwissentlich auf einer gefälschten Website eingibt. Kurz gesagt: Die Einführung von MFA gehört heute zu den wirksamsten Methoden zum Schutz vor Kontenübernahmen und Datenlecks in Organisationen.

## 3. Vergleich zwischen MFA für Verbraucher und Unternehmen

Bevor man über die Implementierung von Multi-Faktor-Authentifizierung (MFA) nachdenkt, ist es wichtig, die Unterschiede zwischen der MFA zu verstehen, die von Verbrauchern genutzt wird (z. B. beim Login in E-Mail-Konten, soziale Netzwerke oder Online-Banking), und der MFA, die in Unternehmens- oder institutionellen Umgebungen eingesetzt wird. Auch wenn das Grundprinzip dasselbe ist, unterscheidet sich der Kontext der Nutzung von MFA für Verbraucher und Unternehmen in mehreren wesentlichen Punkten.

| Aspekt | MFA für Verbraucher | MFA für Unternehmen |
|---|---|---|
| **Initiative zur Einführung** | Freiwillig. Der Nutzer aktiviert MFA selbst, um die Sicherheit seines Kontos zu erhöhen. | Vorgabe von oben. Die Organisation muss MFA einführen, um das Sicherheitsniveau zu erhöhen und regulatorische Anforderungen zu erfüllen. |
| **Verpflichtung** | In der Regel aktiviert der Nutzer MFA freiwillig. Ausnahme sind z. B. Banken, bei denen MFA gesetzlich vorgeschrieben ist. | Durch Sicherheitsrichtlinien vorgeschrieben. Jeder Mitarbeitende muss MFA beim Login in ausgewählte Systeme verwenden. |
| **Authentifizierungs-methoden** | Begrenzte, einfache Methoden: meist SMS, E-Mail oder Authenticator-App (TOTP). Hardware-Keys und Passkeys sind seltener. | Breite Auswahl: SMS/TOTP, Push-Benachrichtigungen, FIDO-Keys, Passkeys, QR-Codes und weitere. Die Auswahl richtet sich nach den Bedürfnissen der Organisation. |
| **Verwaltung** | Keine zentrale Verwaltung. Jeder Dienst bietet eigene MFA-Funktionen, die der Nutzer für jedes Konto separat konfigurieren muss. | Zentrale Verwaltung, z. B. über eine Administrationskonsole. Einheitliche MFA-Lösung für alle Mitarbeitenden, typischerweise integriert in ein Benutzerverzeichnis (z. B. Active Directory). Administratoren können Richtlinien durchsetzen und die Nutzung überwachen. |
| **Support und Wiederherstellung** | Eingeschränkt. Bei Verlust des zweiten Faktors (z. B. Telefon) hängt der Nutzer vom Support des jeweiligen Dienstes ab. | Ausgeprägt. Organisation definiert interne Prozesse für die Wiederherstellung des Zugangs, z. B. Ausgabe von Ersatzschlüsseln, Support durch die IT-Abteilung, Notfallcodes oder mehrere erlaubte Authentifizierungsmethoden. |
| **Skalierung** | Ein einzelner Nutzer schützt einige wenige Konten. | Großflächige Skalierung. Einführung für Dutzende, Hunderte oder Tausende Mitarbeitende und Unternehmenssysteme. |
| **Ziele und Schutzumfang** | Schutz personenbezogener Daten des Nutzers (E-Mail, Profile in sozialen Medien, Finanzdaten) vor unbefugtem Zugriff. | Schutz der Ressourcen der Organisation (Daten in internen Systemen, Geschäftsanwendungen, Cloud-Dienste) sowie Erfüllung von |

| | | |
|---|---|---|
| | | Sicherheitsanforderungen, zum Beispiel Empfehlungen aus Audits oder Compliance-Vorgaben.<br><br>MFA ist häufig Teil einer umfassenderen Sicherheitsstrategie im Unternehmen. |
| **Beispiele für Implementierungen** | Dienste wie Gmail oder Facebook, bei denen der Nutzer MFA selbst aktiviert und konfiguriert.<br><br>Zugang zum Online-Banking erfolgt meist über Passwort und einmaligen SMS-Code. | Zugriff auf das Firmennetzwerk erfordert Passwort und Bestätigung in der mobilen App.<br><br>Administratorzugang zu kritischen Servern wird zusätzlich durch FIDO-Hardware-Schlüssel abgesichert.<br><br>Mitarbeitende melden sich bei Unternehmensanwendungen an, indem sie MFA verwenden, zum Beispiel einen Code vom Telefon oder eine Push-Benachrichtigung. |

Die Einführung von MFA in Unternehmensumgebungen ist deutlich komplexer als die einfache Aktivierung von MFA durch einen einzelnen Endverbraucher. In einer Organisation müssen mehrere Aspekte berücksichtigt werden:

- Auswahl einer geeigneten technischen Lösung, die die Sicherheitsanforderungen erfüllt und sich in die bestehende IT-Infrastruktur integriert.
- Ein strukturierter Implementierungsprozess, der in Phasen abläuft und Betriebsunterbrechungen minimiert.
- Sicherstellung des laufenden Betriebs der Lösung, zum Beispiel Benutzerverwaltung, Gerätezyklen und Gewährleistung der Betriebsfähigkeit.

Dieser Leitfaden konzentriert sich auf eine organisierte, zentral gesteuerte Implementierung von MFA in einer Organisation.

**Erfahren Sie, wie Rublon MFA die Einhaltung von Vorschriften unterstützt, den Zugriff auf Daten schützt und sich mit geschäftskritischen IT-Systemen integriert.**
**Entdecken Sie konkrete Anwendungsfälle in unterschiedlichen organisatorischen Umgebungen.**

# 4. Auswahl eines MFA-Anbieters – worauf sollte man achten?

Der erste Schritt bei der Implementierung von MFA ist die Auswahl einer geeigneten Lösung und eines passenden Anbieters. Auf dem Markt sind viele MFA-Plattformen verfügbar. Entscheidend ist daher die Wahl eines Systems, das die Anforderungen der Organisation in Bezug auf Sicherheit, Compliance, Funktionalität und Benutzerfreundlichkeit erfüllt.


Die Auswahl eines MFA-Anbieters ist eine strategische Entscheidung, denn die gewählte Lösung wird ein zentrales Element der Sicherheitsinfrastruktur darstellen.Daher sollte ausreichend Zeit für eine sorgfältige Bewertung jeder Lösung eingeplant werden. Man sollte sich nicht ausschließlich von Preis oder Markenbekanntheit leiten lassen, entscheidend ist die Anpassung an die spezifischen Anforderungen der Organisation. Im Folgenden erläutern wir die wichtigsten Kriterien für die Auswahl eines MFA-Anbieters.

## 4.1. Sicherheit und Einhaltung von Standards

Es ist wichtig sicherzustellen, dass die MFA-Lösung bewährte kryptografische Mechanismen zur Absicherung der Authentifizierungsdaten verwendet, zum Beispiel Geheimnisse und Schlüssel oder zeitbasierte Einmalpasswörter entsprechend der Spezifikation RFC 6238. Private Schlüssel sollten in einem sicheren Modul gespeichert werden. Der Anbieter sollte die Einhaltung von Branchenstandards wie FIDO2 (moderne, phishing-resistente Authentifizierung) gewährleisten und Zertifikate zur Bestätigung der Konformität mit Normen bereitstellen, zum Beispiel ISO 27001 für Informationssicherheit. Der Anbieter sollte die Einhaltung von Branchenstandards wie FIDO2 (moderne, phishing-resistente Authentifizierung) gewährleisten und Zertifikate zur Bestätigung der Konformität mit Normen bereitstellen, zum Beispiel ISO 27001 für Informationssicherheit.

Es ist ratsam zu prüfen, ob der Anbieter die Implementierung einer phishing-resistenten MFA ermöglicht. Methoden, die den Standards FIDO U2F oder FIDO2 entsprechen, gelten heute als Goldstandard der Sicherheit.Lösungen, die ausschließlich veraltete oder anfällige Methoden bereitstellen, sollten vermieden werden, zum Beispiel SMS-Codes oder ausschließlich TOTP.Nicht alle Formen von MFA bieten das gleiche Sicherheitsniveau. Besonders grundlegende MFA-Varianten, die auf SMS basieren, sind anfällig für Angriffe wie den SIM-Tausch (eng. *SIM swap*).

**Erfahren Sie, wie Rublon MFA dabei hilft, Sicherheits- und Compliance-Anforderungen zu erfüllen.**

## 4.2. Unterstützte Authentifizierungsmethoden

Es ist wichtig zu prüfen, welche MFA-Methoden ein Anbieter unterstützt und ob diese zu den Anforderungen der Organisation passen. Das Mindestset besteht in der Regel aus: Einmalpasscodes (OTP) in der mobilen App, SMS-Codes und Push-Benachrichtigungen auf das Telefon. Immer häufiger wird auch die Unterstützung für FIDO-U2F- und FIDO2-Sicherheitsschlüssel (z. B. YubiKey) sowie für hardware- oder softwarebasierte Passkeys erwartet, die beispielsweise auf dem Computer des Mitarbeiters oder in dessen Google Password Manager gespeichert sind.

Gute MFA-Plattformen ermöglichen die Verwaltung von Richtlinien zur Auswahl der Methoden.Dadurch kann die Organisation stärkere, phishingresistente Methoden für Administratoren erzwingen und gleichzeitig für andere Mitarbeiter Methoden mit geringerem Risiko zulassen (z. B. SMS-Codes für Nutzende ohne Smartphone, die sich in Anwendungen anmelden, in denen keine sensiblen Daten gespeichert werden). Dieses Vorgehen schafft ein Gleichgewicht zwischen Sicherheit und Benutzerfreundlichkeit.

Rublon MFA ermöglicht beispielsweise die gleichzeitige Nutzung verschiedener Methoden, von Push-Benachrichtigungen über die Anmeldung mit FIDO2-Schlüsseln bis hin zu TOTP-Codes. Dadurch

kann die MFA-Strategie flexibel an unterschiedliche Risikostufen und Benutzertypen angepasst werden.

**Erfahren Sie, welche Authentifizierungsmethoden Rublon MFA unterstützt.**

Flexibilität bei der Auswahl der Methoden ist ebenfalls wichtig. Unterschiedliche Szenarien (Anmeldung über VPN, Zugriff auf E-Mail-Dienste in der Cloud, Remote-Zugriff auf Windows- und Linux-Systeme usw.) können unterschiedliche Authentifizierungsmethoden erfordern. Es ist daher empfehlenswert zu prüfen, ob die betrachtete Lösung diese Flexibilität bietet und ob mehrere Geräte für ein Konto registriert werden können (z. B. eine App auf dem Firmen- und dem Privattelefon als Backup sowie ein FIDO-Schlüssel).


## 4.3. Integration in die bestehende Infrastruktur

Eine MFA-Lösung funktioniert nicht isoliert, sondern muss mit den Systemen und Anwendungen integriert werden, die eine Organisation schützen möchte. Deshalb sollte geprüft werden, ob der Anbieter die in der Organisation verwendeten Technologien unterstützt, zum Beispiel:

- Import und Synchronisierung von Benutzerkonten aus Verzeichnisdiensten wie Active Directory oder Entra ID.

- Unterstützung der Protokolle SAML, LDAP und RADIUS zur Integration mit Webanwendungen und VPN-Netzwerken.
- Unterstützung von **Single-Sign-On-Diensten**.
- Native Konnektoren für Microsoft-Technologien wie Windows Logon, RDP, Remote Desktop Gateway, Remote Desktop Web Access, Remote Desktop Web Client, Outlook Web App (OWA) und Active Directory Federation Services (AD FS).

Je mehr Technologien, Protokolle und native Integrationen eine MFA-Lösung unterstützt, desto einfacher lässt sie sich in einer Organisation implementieren. Außerdem sollte geprüft werden, ob der Anbieter APIs und fertige SDK-Bibliotheken bereitstellt. Solche Werkzeuge sind hilfreich, wenn eine Organisation MFA in eigene Geschäftsanwendungen oder Kundenportale einbinden möchte.

Ein Beispiel für eine flexible Lösung ist Rublon MFA, das fertige Konnektoren für Microsoft-Dienste (u. a. AD FS, OWA, Windows Logon, RDP), Integrationen für SAML und RADIUS sowie ein REST-API für die Einbindung von MFA in eigene Web- und Mobile-Anwendungen bietet.

**Erfahren Sie mehr darüber, wie Rublon MFA sich in Windows, Active Directory, SAML, LDAP, RADIUS und andere Systeme integriert.**

## 4.4. Einfaches Benutzer- und Gerätemanagement

Einer der wichtigsten Aspekte bei der Auswahl einer MFA-Lösung ist die einfache Verwaltung des Lebenszyklus von Benutzern und ihren Authentifizierungsmethoden. Es sollte geprüft werden, ob die Plattform eine automatische Benutzerregistrierung ermöglicht, sodass neue Benutzer beim ersten erfolgreichen Login mit der gesicherten Technologie automatisch zur Plattform hinzugefügt werden. Wenn der Anbieter eine Verzeichnissynchronisierung unterstützt, sollte auch geklärt werden, ob neue Konten aus der Domäne unmittelbar nach der Synchronisierung in der MFA-Plattform erscheinen.

Wichtig ist ebenfalls, wie der Registrierungsprozess für neue Geräte (eng. *device enrollment*) aussieht, die Benutzer verwenden möchten.Dabei geht es darum, ob die Registrierung selbstständig über ein benutzerfreundliches Geräteportal erfolgen kann oder ob ein Administrator manuell eingreifen muss. Die Möglichkeit, Benutzern eine E-Mail mit einem Link zur Geräteregistrierung zu senden, ist eine besonders komfortable Lösung.

**Erfahren Sie, wie Rublon Benutzerkonten automatisch mit Active Directory und Entra ID synchronisiert (Directory Sync).**

## 4.5. Benutzerfreundlichkeit

MFA fügt dem Anmeldeprozess einen zusätzlichen Schritt hinzu. Daher sollte sichergestellt werden, dass dieser Schritt für Mitarbeitende nicht zu umständlich ist. Es lohnt sich, die Benutzerfreundlichkeit der angebotenen Methoden zu vergleichen und dabei folgende Fragen zu berücksichtigen:

- Ist die mobile App des Anbieters intuitiv, in deutscher Sprache verfügbar und mit gängigen mobilen Betriebssystemen kompatibel?
- Können Push-Benachrichtigungen mit einer einzigen Berührung bestätigt werden und besteht die Möglichkeit, sie zusätzlich per Fingerabdruck oder Gesichtsscan abzusichern?
- Ist die Benutzeroberfläche der Anmeldung einheitlich gestaltet, lässt sie sich an Unternehmensvorgaben anpassen und unterstützt sie unterschiedliche Authentifizierungsmethoden für verschiedene technische Voraussetzungen und Benutzergruppen?

Je einfacher und verständlicher der Authentifizierungsprozess für Endnutzer ist, desto geringer ist der Widerstand bei der Einführung. Es ist sinnvoll, beim Anbieter nach Schulungs- und Informationsmaterialien für Mitarbeitende zu fragen — etwa Dokumentationen, Schritt-für-Schritt-Anleitungen oder Demo-Videos. Solche Materialien erleichtern die Einführung und den laufenden Betrieb der Lösung erheblich.

**Erfahren Sie, wie die Funktion „Gerät speichern“ in Rublon MFA die Benutzerfreundlichkeit erhöht.**

## 4.6. Technische Anforderungen und Skalierbarkeit

Bei der Auswahl eines MFA-Systems sollte die zugrunde liegende Architektur sorgfältig bewertet werden:

- Handelt es sich um einen lokalen Anbieter, der den nationalen Markt und die Anforderungen der Kunden kennt?
- Ist es eine lokale Lösung (on-premises) oder ein Cloud-Dienst im Modell „Software as a Service“ (SaaS)?
- Wenn es ein Cloud-Dienst ist: Werden die Daten innerhalb der Europäischen Union gespeichert? Dies kann für die Einhaltung regulatorischer Vorgaben entscheidend sein.
- Welche Hardwareanforderungen bestehen? Wie sieht die Systemkompatibilität aus und werden zusätzliche Server benötigt (z. B. Proxy-Server)?
- Kann die Lösung mit der erwarteten Zahl an Nutzern und Anmeldungen umgehen — etwa mit hunderten parallelen Authentifizierungen während Spitzenzeiten?

- Lässt sich das System problemlos erweitern, z. B. um zusätzliche Anwendungen, Benutzer, Sicherheitsrichtlinien und Authentifizierungsmethoden, wenn die Anforderungen der Organisation wachsen?

**Erfahren Sie, welche technischen Anforderungen Rublon MFA erfüllt.**

## 4.7. Audit und Compliance

Für Organisationen ist es entscheidend nachvollziehen zu können, wer, wann, wo und von welchem Gerät sich mit MFA anmeldet. Daher sollte geprüft werden, ob die Plattform Authentifizierungs-Logs bereitstellt, die für weitere Analysen exportiert werden können, zum Beispiel in SIEM-Lösungen.

Zusätzlich sollte im Hinblick auf die Einhaltung von Vorschriften geprüft werden, ob die Lösung des Anbieters die Anforderungen allgemeiner Sicherheitsregulierungen erfüllt, wie etwa der DSGVO, der NIS2-Richtlinie oder des nationalen Cybersicherheitsgesetzes. Darüber hinaus können je nach Branche spezifische Vorgaben relevant sein. Für Finanzinstitute sind dies beispielsweise die DORA-Verordnung sowie die Richtlinien der nationalen Finanzaufsicht (BaFin). Im öffentlichen Sektor spielen zudem Empfehlungen und Zertifizierungen nationaler Institutionen eine wichtige Rolle, wie etwa die Zertifizierungen von BSI oder Listen mit empfohlenen Softwarelösungen. Es ist außerdem ratsam zu prüfen, ob das betreffende MFA-Produkt bereits in anderen Institutionen erfolgreich eingesetzt wird.

**Erfahren Sie, wie Authentifizierungs-Logs, Auditfunktionen und Telefonie in Rublon MFA funktionieren.**

## 4.8. Technischer Support und Kosten

Bei der Auswahl einer MFA-Lösung ist es wichtig, den angebotenen Support des Anbieters zu bewerten. Schnelle Hilfe bei Problemen oder Fragen ist von großem Wert. Daher sollte überprüft werden, ob der technische Support während der üblichen Geschäftszeiten in Deutschland verfügbar ist. Ebenso relevant ist die Bereitstellung von Unterstützung in deutscher Sprache, da dies die Kommunikation erheblich erleichtert und beschleunigt.

Neben dem technischen Support spielen auch die Kosten der Lösung eine wesentliche Rolle. Es empfiehlt sich, das Lizenzmodell sowie die Gesamtkosten zu analysieren und mit der Qualität der Lösung in Relation zu setzen. Die günstigste Variante ist nicht immer die optimale. Entscheidend ist, dass die Lösung zu den finanziellen Möglichkeiten der Organisation passt. Die Kosten können pro Nutzer oder pro Lizenz berechnet werden und als monatliche oder jährliche Abonnementgebühren anfallen. Teilweise werden auch mehrjährige oder sogar unbefristete Lizenzen angeboten – es lohnt

sich zu prüfen, wie dies beim jeweiligen Anbieter gestaltet ist und welche langfristigen Auswirkungen dies hat.

Es ist zu beachten, dass bei der Analyse auch versteckte Kosten berücksichtigt werden sollten, zum Beispiel:

- Kosten für den Kauf zusätzlicher Geräte (FIDO-Schlüssel, Diensttelefone)
- Telekommunikationsgebühren für Authentifizierungsmethoden, die auf Telefondiensten basieren (zum Beispiel SMS)
- Kosten für den Betrieb von On-Premises-Servern (Kosten für Hardware und Administration)

**Erfahren Sie, wie das Abonnementmodell in Rublon MFA funktioniert.**

## 4.9. Praktische Checkliste: Auswahl eines MFA-Anbieters

Nachfolgend finden Sie eine kurze Checkliste mit den wichtigsten Fragen, die man bei der Auswahl eines MFA-Anbieters stellen sollte. Sie kann als Kontrollliste während der Analyse verschiedener Angebote verwendet werden:

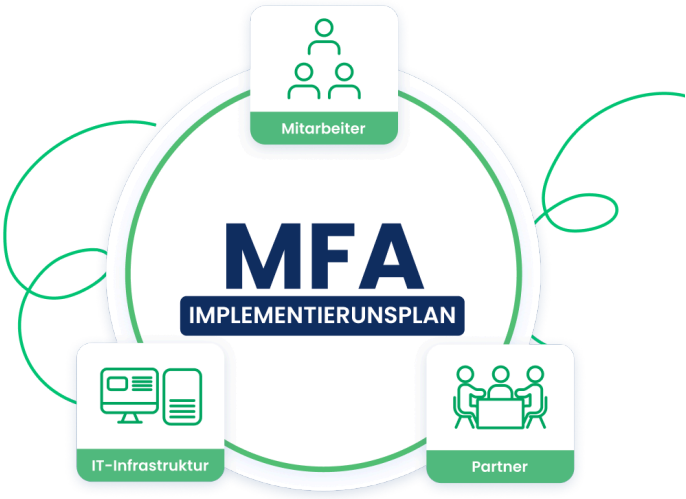
- Erfüllt die Lösung die erforderlichen Sicherheitsstandards (FIDO2, AAL2/AAL3, Push) und bietet sie Widerstandsfähigkeit gegen typische Angriffe im Internet (Phishing, Ransomware, Abfangen von Codes)?
- Welche Authentifizierungsmethoden unterstützt der Anbieter? Stimmen sie mit unseren Anforderungen überein? Unterstützt er FIDO-Hardware-Schlüssel, Push-Benachrichtigungen, SMS-Codes, E-Mail-Codes, QR-Codes, Offline-Codes usw.?
- Integriert sich die Lösung mit unserem lokalen Active Directory, Entra ID, RADIUS, LDAP, SAML, SSO sowie mit unseren wichtigsten Systemen (VPN, E-Mail, Business-Anwendungen)? Bietet sie eine API/SDK für nicht standardisierte Integrationen?
- Wie funktioniert die Verwaltung von Benutzern und Authentifizierungsgeräten? Gibt es eine Synchronisierung von Benutzern, Self-Service-Geräteregistrierung, einfache Reset- und Wiederherstellungsprozesse?
- Sind Benutzeroberfläche und Abläufe der Authentifizierung benutzerfreundlich? (Mobile App, deutsche Sprache, einfache Nutzung, Unterstützung für unterschiedliche Gerätetypen der Benutzer?)
- Passt die Architektur der Lösung zur Infrastruktur unserer Organisation? Was sind die Systemanforderungen und kann die Lösung hohe Leistung und Verfügbarkeit bei der erwarteten Benutzerzahl gewährleisten?
- Welche Audit-Möglichkeiten bietet der Anbieter? Können Ereignisprotokolle in SIEM-Lösungen integriert werden? Hilft die Lösung, regulatorische Anforderungen zu erfüllen, die für unsere Organisation gelten?

- Wie sehen die Lizenz- und Betriebskosten aus? Sind alle Komponenten berücksichtigt (z. B. Kauf von physischen Schlüsseln, eventuelle SMS-Kosten)? Wie schnell reagiert der technische Support (Verfügbarkeit)?
- Hat der Anbieter nachweislich positive Kundenmeinungen, insbesondere im öffentlichen Sektor oder in einer Branche, die unserer ähnelt? Wird die Lösung von anerkannten Institutionen geprüft oder genutzt?

**Erfahren Sie, warum Unternehmen in Deutschland Rublon MFA als ihre vertrauenswürdige Lösung für Multi-Faktor-Authentifizierung wählen.**

# 5. Vorbereitung der Organisation auf die Einführung von MFA

Die Vorbereitung der Organisation auf die Einführung von MFA betrifft sowohl die technische als auch die organisatorische Seite. Die Einführung der Multi-Faktor-Authentifizierung ist ein Projekt, das sowohl das IT-Team als auch gewöhnliche Mitarbeitende, Führungskräfte sowie oft auch externe Partner und Integratoren einbindet. Eine gute Vorbereitung minimiert das Risiko zukünftiger Probleme und Chaos während des ersten Starts der MFA-Lösung. Je mehr potenzielle Probleme im Voraus gelöst werden, desto reibungsloser verläuft die Implementierung.




Nachfolgend finden Sie die wichtigsten Schritte zur Vorbereitung der Organisation auf die Einführung von Multi-Faktor-Authentifizierung.

**Erfahren Sie, welches die Best Practices für die Einführung von Rublon MFA sind.**

## 5.1. Unterstützung durch die Geschäftsleitung einholen und Sicherheitsrichtlinien festlegen

Falls dies noch nicht geschehen ist, sollte den Entscheidungsträgern die geschäftliche Begründung für die Einführung einer MFA-Lösung präsentiert werden, z. B.:

- Erfüllung regulatorischer Anforderungen.
- Verringerung des Risikos von Datenlecks.

- Aufzeigen von Sicherheitsvorfällen und Angriffsarten, denen die MFA-Lösung vorbeugen kann.
- Hervorheben der Vorteile dieser Lösung im Vergleich zu anderen.

Die Unterstützung durch die Geschäftsleitung erleichtert die Durchsetzung der Veränderungen und die spätere Kommunikation. Parallel dazu sollte eine interne Sicherheitsrichtlinie ausgearbeitet oder aktualisiert werden, die den Einsatz von MFA definiert, unter anderem:

- Welche Systeme und Ressourcen von MFA abgedeckt werden?
- Für wen MFA gelten wird (gilt MFA sofort für alle Mitarbeitenden oder zunächst nur für die Verwaltung und besonders gefährdete Bereiche)?
- Welche Methoden zulässig und welche untersagt sein sollen (z. B. kann festgelegt werden, dass SMS-Methoden vorübergehend akzeptabel sind, langfristig jedoch eine Migration zu einer mobilen App oder FIDO-Schlüsseln erforderlich ist)?
- Wann MFA gemäß den oben genannten Richtlinien endgültig verpflichtend eingeführt wird?

„Die Einführung von MFA ist eine strategische Investition in die Cyberresilienz einer Organisation. Der Erfolg eines solchen Projekts erfordert das aktive Engagement der Geschäftsleitung sowie eine kohärente, klar definierte Sicherheitsrichtlinie. Ohne diese Grundlagen führt selbst die modernste Technologie nicht zu einer realen Stärkung des Schutzes von Daten und Diensten."

**Michał Wendrowski, Vorstandsvorsitzender der Rublon sp. z o.o.**

## 5.2. Inventarisierung der Systeme und Analyse der Anforderungen

Es ist notwendig, eine Liste aller Systeme, Anwendungen und Dienste zu erstellen, in denen die Einführung von MFA geplant ist, zusammen mit Informationen darüber, wie dies umzusetzen ist. In diesem Stadium wissen wir bereits, dass die Einführung möglich ist. Jetzt müssen wir so viele konkrete Informationen wie möglich zu den genauen Schritten des Rollouts sammeln. Entscheidend ist die Zusammenarbeit mit dem MFA-Anbieter oder Integrator, um die MFA-Konfiguration für alle in der Organisation benötigten Ressourcen zu planen.

Für jeden identifizierten Bereich ist festzustellen, wie MFA technisch eingeführt werden soll:

- Gibt es auf der Website des Anbieters eine Integrationsdokumentation?
- Ist eine Integration über das Protokoll RADIUS/LDAP/SAML erforderlich?
- Ist der Einsatz eines Agents/Konnektors erforderlich (z. B. eines RADIUS-Proxys für VPN)?

- Ist die Installation eines Moduls/Konnektors/Plugins erforderlich?
- Ist eine automatisierte Massenausrollung auf vielen Arbeitsstationen oder Servern gleichzeitig möglich?

**Beispiel:** Wenn sich Mitarbeitende mit Remote-Desktops (RDP) verbinden, ist zu prüfen, wie der Zugriff mit der ausgewählten Lösung abgesichert werden kann. Bietet die MFA-Lösung einen dedizierten RDP-Konnektor oder wird die Integration auf andere Weise durchgeführt? Wenn in der Organisation Legacy-Systeme vorhanden sind, die moderne Methoden nicht unterstützen, ist zu prüfen, wie die Lösung deren Absicherung auf anderem Wege ermöglicht (z. B. Zugriff nur über ein mit MFA gesichertes VPN statt direkt).

## 5.3. Vorbereitung der Testumgebung

Bevor MFA in der Produktionsumgebung aktiviert wird, sollte eine Testumgebung vorbereitet werden, die die wichtigsten Elemente der Produktionsinfrastruktur widerspiegelt. Das kann eine separate Instanz des Active Directory mit einigen Testkonten sein sowie geklonte Instanzen der wichtigsten Produktionsanwendungen. Die Installation und Konfiguration der MFA-Lösung unter kontrollierten Bedingungen in der Testumgebung ermöglicht es, Integrationen zu überprüfen (z. B. ob die VPN-Anmeldung mit unserer aktuellen Konfiguration korrekt funktioniert) und sich mit der Funktionsweise und Verwaltung der Lösung vertraut zu machen.

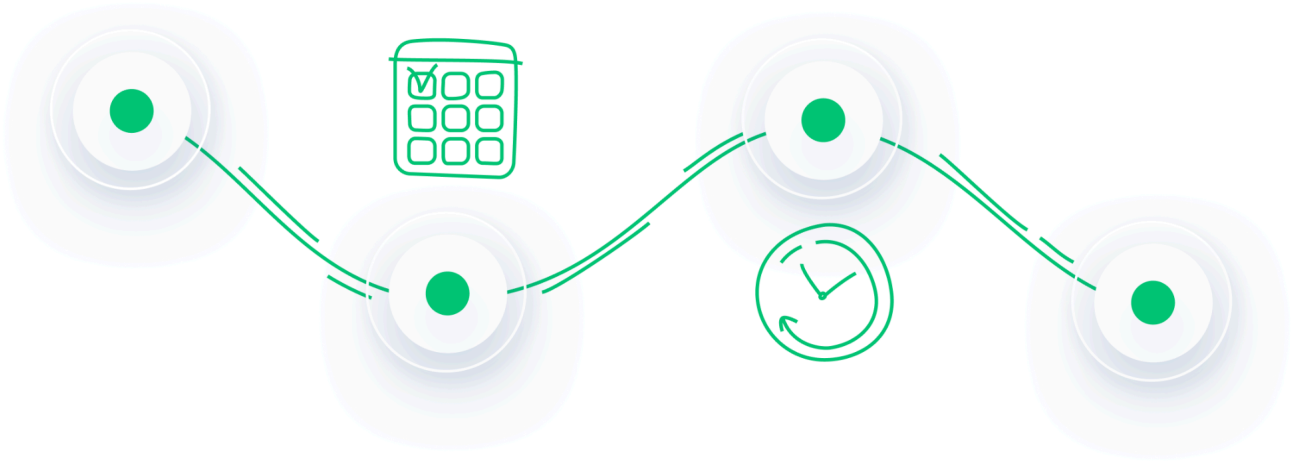
Wenn es nicht möglich ist, eine separate Testumgebung zu erstellen, sollte zumindest der Test mit einer begrenzten Gruppe realer Konten (z. B. der IT-Abteilung) im nicht-störenden Modus in Betracht gezogen werden. Wenn die ausgewählte Lösung die Möglichkeit bietet, MFA nur für ausgewählte Benutzer zu aktivieren, sodass alle anderen weiterhin wie gewohnt ohne spürbare Änderungen arbeiten, sollte dieser Modus während der Tests genutzt werden.

## 5.4. Implementierungszeitplan

Es sollte ein vorläufiger Implementierungszeitplan vorbereitet werden. Bereits in der Vorbereitungsphase lohnt es sich, die einzelnen Phasen der Implementierung grob zu skizzieren. Es müssen Zeiträume für den Pilotbetrieb, für mögliche Konfigurationsanpassungen, für die Kommunikationskampagne sowie für die Unterstützung der Nutzer nach der Einführung eingeplant werden.

Die festgelegten Zeitrahmen sollten realistisch sein und unter anderem Saisonalität berücksichtigen (man sollte kein neues Login-Verfahren kurz vor Feiertagen oder zum Jahresabschluss einführen,

wenn die IT-Abteilung andere Belastungen hat). Wenn eine längere Konfiguration oder Implementierung erforderlich ist (z. B. Installation und Anpassung eines Dienstes), müssen Zeit für Konfiguration und Tests berücksichtigt werden. Der Zeitplan sollte mit den wichtigsten Stakeholdern abgestimmt werden, z. B. mit den Leitern der Abteilungen, deren Mitarbeitende am Pilotprojekt teilnehmen.



## 5.5. Vorbereitung der Ressourcen und Werkzeuge

Es muss sichergestellt werden, dass alle für die Durchführung des Projekts erforderlichen Ressourcen verfügbar sind:

- Die Server und Instanzen für die Installation der MFA-Komponenten sind vorhanden.
- Die Netzwerkverbindungen zwischen den Systemkomponenten sind konfiguriert (z. B. wenn eine Cloud-MFA-Lösung verwendet wird, müssen Firewalls den Verkehr zur Cloud zulassen und Connectoren müssen sich frei mit der Identitätsdatenbank der Benutzer verbinden können).
- Geräte wie FIDO-Sicherheitsschlüssel müssen rechtzeitig bestellt werden, damit sie pünktlich eintreffen und an die Mitarbeitenden verteilt werden können.
- Die technische Dokumentation der Lösung ist griffbereit. Sie sollte bereits vor Beginn der Implementierung durchgesehen und wichtige Abschnitte markiert werden, damit sie während der Konfiguration jederzeit verfügbar ist. Bei Unklarheiten sollte Rücksprache mit dem Anbieter gehalten werden.

## 5.6. Richtlinie für den Umgang mit Ausnahmen und Notfallsituationen

Bereits in der Planungsphase sollte festgelegt werden, welche Ausnahmen von der MFA-Pflicht zulässig sind und in welchen Situationen. Es sollte auch überlegt werden, welche Ausnahmen von den globalen MFA-Richtlinien in der Organisation bestehen können. Beispiele:

- Sollten Dienstkonten, externe Benutzer und Gäste von MFA erfasst werden? Wenn ja, auf dieselbe Weise wie reguläre Mitarbeitende, oder sollte ein anderes Vorgehen angewendet werden?
- Soll Mitarbeitenden ohne Diensttelefon die Nutzung privater Telefone erlaubt werden oder sollen sie Methoden verwenden dürfen, die kein Telefon erfordern?

Es lohnt sich, ein Verfahren für den Notfallzugang (engl. *break-glass*) zu dokumentieren, also was zu tun ist, wenn jemand den Zugang verliert (z. B. Telefon verloren, keine Wiederherstellungscodes verfügbar) oder wenn das MFA-System ausfällt. Diese Verfahren werden später im Leitfaden ausführlicher beschrieben, aber bereits jetzt lässt sich ein erster Entwurf planen.

## 5.7. Informationskampagne und Schulungsmaterialien

Die Einführung von MFA betrifft viele Mitarbeitende, daher ist es entscheidend, sie angemessen zu informieren und zu schulen. Bereits in der Vorbereitungsphase sollte festgelegt werden, wann und wie die bevorstehenden Änderungen kommuniziert werden. Es lohnt sich auch, den MFA-Anbieter zu fragen, ob er fertige Materialien für die Kommunikation mit Endbenutzern bereitstellt.

Eine gute Praxis ist es, eine interne Liste häufig gestellter Fragen und Antworten sowie Anleitungen für Mitarbeitende vorzubereiten, zum Beispiel einen kurzen Leitfaden „So richtest du dein Authentifizierungsgerät für MFA Schritt für Schritt ein“. Es kann ausreichen, die vom MFA-Anbieter bereitgestellten Materialien zu nutzen, dennoch ist die Erstellung interner Anleitungen, die an die in der Organisation verwendeten Anwendungen angepasst sind, oft eine gute Idee.

Es kann hilfreich sein, kurze Schulungspräsentationen für Mitarbeitende zu erstellen, die erklären, warum die Organisation MFA einführt (mit Betonung auf den Schutz der Mitarbeitendenkonten und Unternehmensdaten) und wie der neue Anmeldeprozess aussehen wird.

Es empfiehlt sich, verschiedene Kommunikationskanäle für die Mitarbeitenden zu nutzen: E-Mail der IT-Sicherheitsabteilung, Ankündigung im Intranet, ein Q&A-Webinar für Mitarbeitende, Poster im Büro usw. Einige Materialien können direkt vom MFA-Anbieter stammen (es lohnt sich, nach fertigen Kommunikationsvorlagen, Grafiken oder kurzen Leitfäden zu fragen). Dann müssen diese nur noch an die internen Gegebenheiten angepasst werden (z. B. Hinzufügen von Unternehmensinformationen, wohin man sich bei Fragen wenden kann).

## 5.8. Schulung des IT-Supportteams

Es ist wichtig, das IT-Supportteam auf die bevorstehende Einführung vorzubereiten. Mitarbeitende des First-Level-Supports müssen die MFA-Mechanismen kennen, um die Benutzer effektiv unterstützen zu können. Daher sollte für sie eine dedizierte Schulung zum neuen System organisiert werden, unter anderem zu folgenden Themen: wie Benutzer und ihre Geräte registriert werden, wie das Notfallkonto verwendet wird, wie die Identität eines anrufenden Mitarbeiters überprüft wird, bevor MFA deaktiviert wird (um keine sozialtechnische Sicherheitslücke zu schaffen).

Eine gute Praxis ist die Erstellung von Verfahren zur Bearbeitung typischer Anfragen wie: *„Ich habe mein Telefon verloren“*, *„Ich kann mich nicht anmelden“*, *„Ich erhalte keinen SMS-Code“*, *„Die mobile App zeigt einen falschen Code an“* usw.

Ebenfalls sinnvoll ist die Benennung mehrerer Personen im Unternehmen (am besten aus der IT- oder Sicherheitsabteilung), die zusätzliches Fachexpertise-Support leisten, schwierigere Fragen beantworten und während der Einführung Hinweise der Benutzer entgegennehmen.

**Erfahren Sie, wie Sie die Rublon-MFA-Plattform in der Administrationskonsole verwalten.**

## 5.9. Praktische Checkliste: Vorbereitung der Organisation auf die MFA-Einführung

Unten finden Sie eine kurze Checkliste zur Vorbereitung Ihrer Organisation auf die Einführung von MFA. Erst wenn die untenstehenden Punkte erfüllt sind, sollte zur eigentlichen Einführung von MFA in der Produktionsumgebung übergegangen werden.

- **MFA-Richtlinie und Umfang der Einführung:**
  - Die Geschäftsleitung hat die Einführung von MFA genehmigt.
  - Es wurde festgelegt, welche Systeme und welche Benutzer von MFA betroffen sein werden.
  - Der Termin für die MFA-Einführung wurde definiert.

- **Liste der Systeme und Integrationen:**
  - Eine Inventarisierung der Anwendungen/Dienste, die durch MFA geschützt werden sollen, wurde erstellt.
  - Die technischen Integrationsmöglichkeiten für jede Position wurden überprüft (bei fehlenden Optionen wurde ein Alternativplan definiert).

- **Tests:**

- Eine Testumgebung für die Probeinstallation und -konfiguration von MFA wurde vorbereitet.
- Erste Integrationstests in kontrollierten Bedingungen wurden geplant.

- **Projektplan und Zeitplan:**
  - Die Einführungsphasen wurden festgelegt (Pilot, Kommunikation, stufenweise Migration, Go-Live).
  - Zeitrahmen und wichtige Termine wurden geschätzt.
  - Verantwortlichkeiten für die Aufgaben wurden verteilt.

- **Sicherstellung technischer Ressourcen:**
  - Die notwendige Infrastruktur (Server, Software) ist verfügbar.
  - Benötigte Geräte wurden bestellt (z. B. Hardware-Schlüssel).
  - Es wurde überprüft, dass die Netzwerkeinstellungen und die Konfiguration eine reibungslose Einführung ermöglichen (z. B. offene Ports, hinzugefügte Ausnahmen in Firewalls).

- **Ausnahme- und Notfallverfahren:**
  - Ein Verfahren für privilegierte Konten, Servicekonten und Situationen wie den Verlust eines Telefons wurde ausgearbeitet.
  - Notfallkonten für Administratoren wurden festgelegt.

- **Kommunikations- und Schulungsmaterialien:**
  - Mitteilungen an Mitarbeitende wurden vorbereitet (E-Mails, Aushänge).
  - Benutzeranleitungen wurden erstellt (oder die vom Anbieter bereitgestellten Vorlagen angepasst), um zu erläutern, wie das Authentifizierungsgerät registriert wird und wie MFA genutzt wird.

- **Schulung des IT- und Helpdesk-Teams:**
  - Eine Schulung für das IT-Supportteam zum Umgang mit dem neuen System wurde organisiert.
  - Referenzmaterialien stehen leicht zugänglich zur Verfügung (interne Wissensdatenbank).
  - Benannte Mitarbeitende sind bereit, Fragen der Benutzer zu MFA zu beantworten.

# 6. Durchführung der MFA-Einführung – einzelne Phasen und bewährte Praktiken

Die Einführung von MFA in der Organisation sollte schrittweise und methodisch erfolgen. Nachfolgend wird ein empfohlener Ablauf der Einführung beschrieben, unterteilt in Phasen, zusammen mit bewährten Praktiken für jede von ihnen. Ein schrittweises Vorgehen ermöglicht es, mögliche Probleme im kleinen Umfang (Pilot) zu erkennen, die Konfiguration anzupassen und die Benutzer schrittweise an die neue Form der Authentifizierung zu gewöhnen sowie die Kontinuität des Betriebs sicherzustellen. Konkrete Schritte können an die Spezifik Ihrer Organisation angepasst werden. Eine kleine Organisation kann einige davon verkürzen oder sogar auslassen, aber die allgemeine Regel lautet: Beginnen Sie mit einer kleinen Anzahl von Benutzern, testen Sie, ziehen Sie Schlussfolgerungen, kommunizieren Sie und skalieren Sie erst dann auf das gesamte Unternehmen.

## 6.1. Durchführung des Pilotprojekts

Der erste Schritt der produktiven Einführung sollte ein Pilotprogramm sein. Dabei wird MFA für eine begrenzte Gruppe von Nutzern und Systemen aktiviert, um die Lösung in der Praxis zu testen, Feedback zu sammeln und mögliche Anpassungen vor der globalen Einführung vorzunehmen.

Ein Pilot ermöglicht es, die MFA-Lösung an reale Nutzungsbedingungen anzupassen und technische Feinheiten zu erkennen. Ein gut durchgeführtes Pilotprojekt erleichtert die spätere produktive Einführung deutlich. Zwar verlängert ein Pilot formal die Gesamtdauer des Projekts, doch zahlt sich dieser Zeitaufwand durch eine reibungslosere Einführung im gesamten Unternehmen aus.

**Erfahren Sie, wie Sie Rublon MFA sicher in einer produktiven Umgebung testen können.**

„Ein Pilotprojekt ist der ideale Moment, um potenzielle Probleme bereits im Vorfeld zu identifizieren, bevor sie die gesamte Organisation betreffen. Unsere Erfahrung aus der Einführung von Rublon MFA bei Hunderten von Kunden zeigt, dass eine sorgfältig geplante Testphase eine präzise Anpassung der Methoden und Richtlinien der Multi-Faktor-Authentifizierung an die tatsächlichen Bedürfnisse der Organisation ermöglicht."

**Patryk Suchorowski, IT-Solutions Architect bei Rublon**

Hier sind Empfehlungen und Best Practices für das Pilotprojekt:

- **Auswahl der Pilotgruppe.**Die Pilotteilnehmer sollten sorgfältig gewählt werden. Häufig beginnt man mit Mitarbeitenden aus der IT- und Sicherheitsabteilung, da diese ein höheres technisches Verständnis und ein stärkeres Sicherheitsbewusstsein haben und daher offener für das MFA-Projekt sind. Zusätzlich sollten Vertreter verschiedener Fachbereiche einbezogen werden (z. B. 1–2 Personen aus HR, Finanzen, Marketing). So lässt sich MFA in unterschiedlichen Arbeitskontexten testen. Die Pilotgruppe sollte nicht zu groß sein (ca. 5–10 % der Belegschaft, je nach Unternehmensgröße), aber divers genug, um ein vollständiges Bild zu erhalten. Wichtig ist, dass die Teilnahme freiwillig erfolgt oder zumindest positiv eingestellt ist.

- **Begrenzter Systemumfang.** Im Pilot müssen nicht sofort alle Systeme abgesichert werden. Es empfiehlt sich, 2–3 wichtigste Systeme auszuwählen und dort MFA zu testen. Beispielsweise könnte man die Absicherung des VPN-Zugangs und den Zugriff auf Windows-Computer einbeziehen, während die Absicherung weiterer Anwendungen später erfolgt. Ein kleinerer Umfang erleichtert die Analyse möglicher Probleme und Fehler.

- **Unterstützung und Kommunikation während des Pilots.** Die Pilotnutzer sollten eine dedizierte Unterstützung erhalten, z. B. direkten Kontakt zum Projektteam. Sie sollten ermutigt werden, Fragen, Probleme und Vorschläge zu melden. Eine gute Praxis ist die Einrichtung einer Diskussionsgruppe, in der sich Pilotnutzer austauschen können und das IT-Team schnell reagieren kann.

- **Testszenarien und Ergebnisanalyse.** Im Pilot sollten verschiedene Szenarien getestet werden: Anmeldung aus dem Büro, Anmeldung aus dem Homeoffice, Wechsel der Authentifizierungsmethode, Anmeldung im Offline-Modus (falls unterstützt), Wiederherstellung des Zugangs (z. B. Simulation eines verlorenen Telefons, um die Reaktionszeit des Supports zu prüfen). Nach Abschluss des Pilots sollten Rückmeldungen gesammelt werden: Was hat gefallen, was hat Schwierigkeiten bereitet, fühlen sich die Nutzer besser geschützt?

- **Optimierung der Konfiguration.** Auf Basis der Pilotergebnisse sollten gegebenenfalls Anpassungen an der MFA-Konfiguration vorgenommen werden. Dies kann eine Änderung der Sicherheitsrichtlinien, die Aktivierung zusätzlicher Authentifizierungsmethoden oder eine Verbesserung der Benutzerhinweise beinhalten. Es ist besser, Details im Pilot zu identifizieren und auszubessern, als erst während der großflächigen Einführung auf Probleme zu stoßen.

## 6.2. Erweiterte stufenweise Einführung

Nach dem erfolgreichen Abschluss des Pilotprojekts (die Ziele wurden erreicht, die Benutzer haben die Lösung akzeptiert, die Konfiguration ist optimiert), kann zur Erweiterung der MFA-Einführung auf

weitere Gruppen von Benutzern, Anwendungen und Systeme übergegangen werden. Die stufenweise Einführung ist besonders empfehlenswert für größere Unternehmen, in denen eine breitflächige Einführung auf einmal zu einer Überlastung der IT- und Supportabteilungen führen könnte.

Nachfolgend die wichtigsten Empfehlungen und Best Practices zur stufenweisen Einführung:

- **Einführung nach Risikogruppen.** Es empfiehlt sich, MFA zunächst für die am stärksten gefährdeten Konten einzuführen: IT-Administratoren, Benutzer mit Zugang zu kritischen Daten (z. B. Führungskräfte) oder Mitarbeitende mit erhöhtem Risiko. Dadurch kann MFA zunächst für weniger sensible Abteilungen und Mitarbeitende aktiviert werden. Dies ermöglicht die Konzentration der Unterstützung und der Kommunikation auf kleinere Gruppen, anstatt den gesamten Helpdesk gleichzeitig zu belasten.

- **Einführung nach Anwendungen.** In einigen Organisationen ist eine Einführung nach Anwendungen sinnvoll. Dann wird MFA zuerst für ausgewählte Anwendungen aktiviert und später für weitere. Beispiel: In der ersten Phase Absicherung der VPN-Anmeldung und kritischer Anwendungen, in der zweiten Phase HR- und Finanzsysteme und in der dritten Phase alle übrigen Anwendungen. Dieses Modell bewährt sich, wenn einige Systeme oder Anwendungen geschäftskritischer sind oder Vorrang haben. Wenn eine Anwendung technisch schwieriger in die MFA-Plattform zu integrieren ist, kann sie später implementiert werden, nachdem Erfahrungen mit einfacheren Integrationen gesammelt wurden. Wichtig ist jedoch, die Einführung nicht endlos zu verzögern. Die einzelnen Phasen sollten sich zügig aneinander anschließen.

- **Monitoring der Fortschritte.** Während der stufenweisen Einführung sollten kontinuierlich Metriken überwacht werden:

- Wie viele Benutzer haben sich registriert? Wie viele verwenden MFA aktiv? Steigt die Anzahl fehlgeschlagener Anmeldungen? Es lohnt sich, Mitarbeitende zu identifizieren, die MFA noch nicht aktiviert haben und möglicherweise individuelle Unterstützung benötigen. In dieser Phase sind regelmäßige Berichte für Abteilungsleitende wertvoll, z. B.: *„In Abteilung A nutzen bereits 90 % MFA, in Abteilung B erst 60 %, daher bitten wir um zusätzliche Unterstützung von Ihrer Seite.“* Manchmal reagieren Mitarbeitende erst, wenn ein Vorgesetzter sagt: *„Das ist verpflichtend, bitte erledigen.“*

- **Erweiterung der Einführung.** Mit zunehmenden Fortschritten können weitere Integrationen hinzugefügt werden, z. B. nach erfolgreicher MFA-Absicherung des VPN und der E-Mail-Zugänge kann MFA für Cloud-Anwendungen eingeführt werden.

- **Eliminierung weniger sicherer Methoden.** Wenn zu Beginn aus Komfortgründen weniger sichere Methoden (z. B. SMS) zugelassen wurden, sollte nach der vollständigen Einführung

geplant werden, diese zu reduzieren oder durch sicherere Methoden zu ersetzen. Diese Änderungen sollten jedoch frühzeitig kommuniziert werden. Sie dürfen Mitarbeitenden nicht unvorbereitet treffen, insbesondere diejenigen, die bereits sicherere Alternativen eingerichtet haben.

„Im öffentlichen und regulierten Sektor beobachten wir immer häufiger stufenweise MFA-Einführungen, die mit Konten von kritischer Bedeutung beginnen und mit einer vollständigen Abdeckung aller Benutzer und Systeme enden. Eine solche Strategie ermöglicht es, das operative Risiko zu verringern und gleichzeitig der Organisation Zeit für Anpassungen sowie die Bereitstellung angemessener technischer Unterstützung zu geben."

**Przemysław Kucharzewski, Channel Sales Manager bei Rublon**

## 6.3. Kommunikation und Schulung der Benutzer

Der erfolgreiche Einsatz von MFA hängt in hohem Maße von der Akzeptanz der Lösung durch die Mitarbeitenden ab. Deshalb sind Kommunikation und Schulung entscheidende Elemente der Einführung, die während des gesamten Projekts stattfinden sollten: vor, während und nach der Einführung.

Kommunikation ist ein weiches, aber entscheidendes Element des Einführungserfolgs. Die MFA-Technologie verteidigt sich nicht von selbst. Die Menschen müssen sie verstehen und akzeptieren. Der Aufwand für eine transparente Information und Schulung der Mitarbeitenden zahlt sich durch weniger Probleme und eine höhere Sicherheit aus.

**Erfahren Sie, wie Sie Endbenutzer auf den Einsatz von Rublon MFA vorbereiten – mit bewährten Kommunikationsvorlagen.**

Nachfolgend finden Sie Empfehlungen und bewährte Praktiken für die Kommunikation und Schulung der Mitarbeitenden:

- **Erklärung des „Warum".** Es ist ratsam, die Mitarbeitenden so früh wie möglich über die geplante Einführung von MFA zu informieren. Wichtig ist, dass in den ersten Mitteilungen die Gründe und Vorteile der MFA-Einführung klar hervorgehoben werden, z. B.: „Zum Schutz der Sicherheit unserer Systeme und der Daten unserer Kunden führt das Unternehmen eine zusätzliche Absicherung in Form der Multi-Faktor-Authentifizierung ein. MFA schützt Sie vor den Folgen gestohlener Passwörter. Selbst wenn jemand Ihr Passwort kennt, kann er sich ohne den zweiten Faktor nicht anmelden."

Es lohnt sich, konkrete Beispiele zu nennen (z. B. „In letzter Zeit gab es viele Angriffe, bei denen Passwörter von Mitarbeitenden entwendet wurden. MFA verhindert solche Angriffe.“) oder auf Empfehlungen von Expertinnen und Experten hinzuweisen.

- **Klare Anleitungen zum „Wie“.** Je näher der Einführungstermin rückt, desto wichtiger ist es, den Mitarbeitenden klare Anweisungen zu geben, was genau sie tun müssen. Die Anleitung sollte leicht zugänglich sein, z. B. im Intranet, per E-Mail oder als gedrucktes Merkblatt. Technischen Jargon gilt es zu vermeiden – statt „registrieren Sie den TOTP-Authenticator“ besser: „richten Sie die App für Einmalcodes ein“.

- **Multikanal-Kommunikation.** Menschen nehmen Informationen auf unterschiedliche Weise auf. Daher sollten mehrere Kommunikationskanäle genutzt werden. E-Mails sind die Basis, aber da viele E-Mails untergehen, sollten MFA-Mitteilungen besonders auffallen. Hilfreich können auch Intranet-Ankündigungen, Nachrichten im Firmenchat, gedruckte Aushänge oder Poster mit klaren Botschaften sein, z. B. „*Anmeldung jetzt sicherer – aktivieren Sie MFA bis zum 30. August!*“.

- **Einbindung der Führungskräfte.** Es lohnt sich, die Manager der einzelnen Abteilungen zu bitten, die Botschaft zu verstärken, z. B. indem sie das Thema MFA in ihren Teammeetings ansprechen. Oft nehmen Mitarbeitende die Nachricht ihres direkten Vorgesetzten ernster als eine allgemeine E-Mail der IT-Abteilung. Wenn im Pilotprojekt Personen aus verschiedenen Abteilungen teilgenommen haben, ist es sinnvoll, deren Stimmen in der Kommunikation zu nutzen, z. B. indem man Zitate in Nachrichten an Mitarbeitende einbindet („Frau Kasia aus HR: *Ich hatte Angst, dass es kompliziert ist, aber die Installation und Einrichtung der App hat 2 Minuten gedauert und jetzt fühle ich mich sicherer mit meinem Konto.*“). Ein solcher menschlicher Aspekt kann unentschlossene Mitarbeitende leichter überzeugen.

- **Hervorhebung der Verbindlichkeit und Fristen.** Während im Pilotstadium die Kommunikation mit den Mitarbeitenden eher in einem Ton freiwilliger Motivation erfolgen kann, müssen die Nachrichten bei Annäherung an den Termin des unternehmensweiten Rollouts bereits deutlich machen, dass ab dem festgelegten Datum die Anmeldung ohne MFA nicht mehr möglich ist. Wer MFA nicht zuvor eingerichtet hat, verliert den Zugriff auf die Systeme und muss sich an den Helpdesk wenden, um sein Konto entsperren zu lassen. Eine solche Botschaft mobilisiert die Mitarbeitenden. Gleichzeitig muss gewährleistet sein, dass Unterstützung leicht zugänglich ist. Das ungünstigste Szenario wäre, wenn am Tag des globalen Rollouts Mitarbeitende überrascht würden, die von nichts wissen. Um dies zu vermeiden, sollten mehrere Erinnerungen versendet werden.

- **Praktische Schulungen.** In manchen Fällen – insbesondere für weniger technisch versierte Mitarbeitende – kann eine kurze Schulung sinnvoll sein.Das kann ein Demo-Video sein, in dem

die Einrichtung Schritt für Schritt gezeigt wird, oder ein Onlineseminar, in dem die Gruppe gemeinsam mit dem Moderator die MFA-App installiert und konfiguriert.

- **Materialien zur Erinnerung an Sicherheitsregeln.** Nach der Einführung von MFA lohnt es sich, kurze Hinweise zu guten Sicherheitspraktiken vorzubereiten. Solche edukativen Mitteilungen können direkt nach dem Rollout versendet werden, um richtige Gewohnheiten zu festigen. Beispiele:
  - *„Geben Sie niemals jemandem Ihren Einmalcode – die IT-Abteilung wird Sie niemals danach fragen!"*
  - *„Wenn Sie auf Ihrem Telefon eine Push-Benachrichtigung erhalten, mit der Sie nicht gerechnet haben, akzeptieren Sie sie NICHT, sondern melden Sie den Vorfall an die IT-Abteilung!"*

## 6.4. MFA wird in Produktion genommen

Der Produktionsstart von MFA ist der Moment, in dem MFA für alle im Projekt festgelegten Benutzer und Systeme verpflichtend wird. Ab diesem Tag erfordert die Anmeldung zusätzlich die Eingabe des zweiten Authentifizierungsfaktors. Dies ist der Höhepunkt der Einführung, daher erfordert er besondere Aufmerksamkeit und Vorbereitung.

Nachfolgend wird dargestellt, wie der produktive Start von MFA durchgeführt werden sollte, um die Kontinuität der Abläufe zu gewährleisten und den Stress sowohl im IT-Team als auch bei den übrigen Mitarbeitern zu minimieren.

- **Einführung zum geeigneten Zeitpunkt.** Der Termin sollte genau an die Spezifik der Organisation und die erwartete Ausfallzeit angepasst werden. In großen Unternehmen führt man Änderungen am besten außerhalb der regulären Arbeitszeiten durch (z. B. nachts oder am Wochenende), um die Auswirkungen auf die Benutzer zu minimieren. In kleineren Teams kann man eine Einführung während der Arbeitszeit in Betracht ziehen, sofern alle Schlüsselmitglieder des Implementierungsteams verfügbar sind. Es ist auch notwendig zu überprüfen, ob der ausgewählte Termin nicht mit anderen wichtigen Ereignissen kollidiert (z. B. Monatsabschluss, Einführung eines anderen Systems).

- **Letzte Erinnerung.** Am Tag vor der globalen MFA-Einführung sollte eine weitere Nachricht an alle Mitarbeiter gesendet werden, die daran erinnert, dass MFA ab morgen erforderlich sein wird. Darin sollten nochmals alle wichtigsten Informationen enthalten sein.

- **Unterstützung im Bereitschaftsmodus.** Am Tag der globalen MFA-Einführung sollten zusätzliche Support-Kanäle aktiviert werden, z. B. ein spezieller Kanal im Firmenchat oder eine verlängerte telefonische IT-Bereitschaft. Zuvor vorbereitete Schulungs- und Hilfsmaterialien für den technischen Support sind ebenfalls hilfreich. Wenn das Unternehmen groß und geografisch verteilt ist, sollte sichergestellt werden, dass in jeder Niederlassung eine Person aus der IT geschult ist und vor Ort helfen kann.

- **Überwachung des Systems.** Direkt nach der Aktivierung der MFA-Pflicht sollte die Systemfunktion intensiv überwacht werden.
    - Treten irgendwelche Fehler in den Authentifizierungslogs auf?
    - Ist die Infrastruktur leistungsfähig genug (z. B. ist der Server nicht überlastet, stauen sich die SMS-Warteschlangen nicht)?
    - Sind keine unerwarteten Probleme aufgetreten?
    - Können alle Benutzer ihre Geräte registrieren?
    - Gibt es Benutzer, die sich nicht authentifizieren können?

- **Kommunikation am Tag der Inbetriebnahme.** Am Tag der globalen Aktivierung von MFA sollten Sie eine kurze Nachricht an alle Mitarbeiter senden, zum Beispiel: *„MFA wurde erfolgreich aktiviert. Wir erinnern daran: Ab jetzt ist bei der Anmeldung die Identitätsbestätigung mittels Methode X erforderlich. Wenn Sie auf Schwierigkeiten stoßen, wenden Sie sich bitte an …"*. Wenn irgendwelche globalen Probleme auftreten, müssen die Mitarbeiter sofort darüber informiert werden.

- **Schnelle Reaktion auf Incidents.** Die ersten Stunden und Tage nach der Aktivierung von MFA sind für alle Mitarbeiter die Zeit, in der die meisten Meldungen eingehen. Wichtig ist die richtige Priorisierung dieser Tickets. Situationen, in denen der Benutzer nicht weiß, wie er etwas ausführen soll, sind weniger kritisch als Situationen, in denen sich der Benutzer überhaupt nicht anmelden kann, obwohl er die beschriebenen Schritte korrekt ausgeführt hat und dadurch keinen Zugang zu wichtigen Diensten hat. In Fällen gesperrten Zugangs sollte die höchste Priorität vergeben und sofort in den Notfallmodus gewechselt werden, z. B. durch Generierung temporärer Zugangscodes, die die Kontinuität des Zugangs sicherstellen, bis die IT-Abteilung das Problem behebt. Es lohnt sich auch, eine Incident-Dokumentation zu führen, um später die Ursachen gründlich zu analysieren und erforderliche Konfigurationsanpassungen vorzunehmen.

- **Abschlussmeeting am Ende des Tages.**Gegen Ende des ersten Tages der globalen MFA-Aktivierung lohnt es sich, ein internes Meeting zu organisieren, bei dem folgende Punkte besprochen werden:
    - Was ist gut gelaufen?
    - Welche Probleme sind aufgetreten?

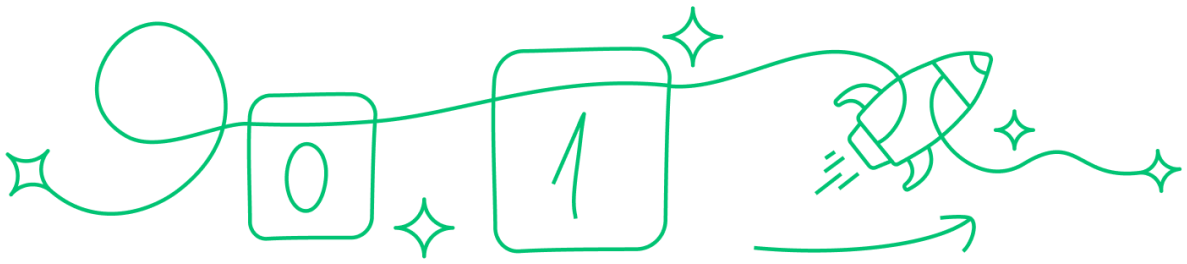
- Wie viele Meldungen wurden bearbeitet?
- Gibt es noch offene Punkte für die kommenden Tage?

- **Kurze Zusammenfassung für die Geschäftsleitung.** ach Abschluss der globalen MFA-Aktivierung sollte der Geschäftsleitung eine kurze Information über den Verlauf der Implementierung übermittelt werden. Eine kurze Nachricht genügt, z. B.: *„Die Implementierung verlief in X % der Fälle erfolgreich, es gab X Probleme, aber alle wurden gelöst (oder es wurde bereits ein Plan zu deren Lösung erstellt).”*. Man kann auch eine positive Nachricht an die gesamte Firma senden, z. B.: *„Glückwunsch, wir haben es gemeinsam geschafft, das Sicherheitsniveau in der Organisation zu erhöhen. Bereits X % von Ihnen nutzen MFA. Vielen Dank für Ihre Zusammenarbeit.”*. Eine solche kurze Nachricht, die an die Mitarbeiter gesendet wird, sorgt dafür, dass sie sich wertgeschätzt fühlen und schließt die MFA-Einführung offiziell ab.

## 6.5. Zeitplan für die MFA-Einführung in der Organisation

Nachfolgend finden Sie einen beispielhaften Zeitplan der Maßnahmen während der globalen Einführung von MFA. Es handelt sich um einen beispielhaften, orientierenden Zeitplan, der an die Gegebenheiten der jeweiligen Organisation angepasst werden sollte.

Die Erstellung eines solchen Zeitplans ermöglicht die Durchführung der MFA-Einführung mit minimalem Risiko. Es ist zu beachten, dass das Ziel darin besteht, dass die Organisation ununterbrochen arbeitet: MFA soll schützen, nicht lahmlegen. Daher sind Elemente wie Notfallcodes oder die Bereitschaft zu einem vorübergehenden MFA-Bypass notwendig, damit die Organisation weiterarbeiten kann. Im Idealfall, mit einem guten Pilotprojekt und guter Kommunikation sowie einer guten MFA-Lösung, sollte der Tag der globalen MFA-Einführung ohne schwerwiegende Zwischenfälle verlaufen.



- **Eine Woche vorher:**
  - Letzte Runde der Kommunikation, die über die bevorstehende Aktivierung der verpflichtenden MFA informiert.
  - Finale Tests der Support-Prozeduren sowie Schulung der IT- und Helpdesk-Teams zur Multi-Faktor-Authentifizierung.

- **Aktivierung der MFA – Tag 0 (Vortag):**
  - Versand einer Mitteilung mit dem Hinweis, dass am nächsten Arbeitstag die MFA aktiviert wird.
  - Überprüfung anhand einiger Testkonten, ob alles wie geplant funktioniert.

- **Aktivierung der MFA – Tag 1 (morgens):**
  - Das IT-Team und der technische Support stehen ab morgens bereit.
  - Aktivierung der MFA gemäß Zeitplan (z. B. um 10:00 Uhr).
  - Versand einer Mitteilung an die Mitarbeitenden, dass die MFA nun aktiv ist.
  - Aktivierung eines verstärkten Support-Bereitschaftsdienstes.

- **Aktivierung der MFA – Tag 1 (mittags):**
  - Überwachung der MFA-Funktionsweise.
  - Regelmäßige Kommunikation zwischen den Teammitgliedern (z. B. stündliche kurze Synchronisation: Anzahl der Meldungen, Arten der Probleme).
  - Feinabstimmung kleiner Einstellungen, sofern erforderlich.

- **Aktivierung der MFA – Tag 1 (Ende des Tages):**
  - Treffen des Projektteams.
  - Besprechung des Tagesverlaufs.
  - Dokumentation der aufgetretenen Probleme und ihrer Lösungen.

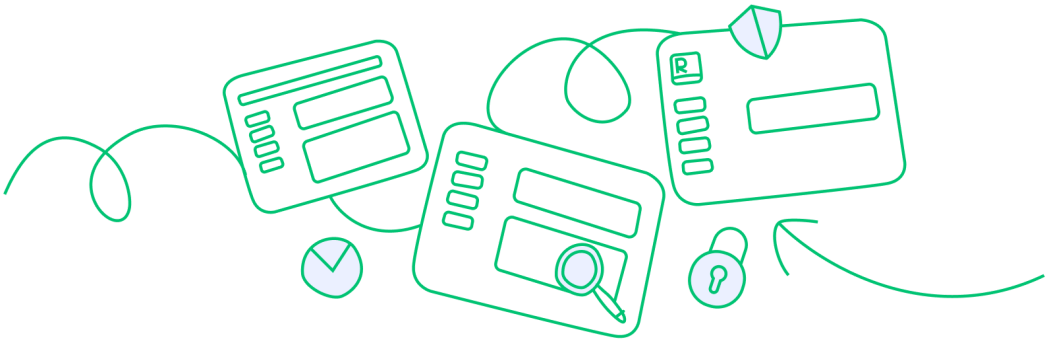
- **Aktivierung der MFA – die folgenden Tage:**
  - Weiterhin erhöhte Support-Bereitschaft.
  - Zusätzliche korrigierende Mitteilungen (falls bestimmte Benutzergruppen weiterhin Probleme mit der neuen Authentifizierungsmethode haben, sollte eine separate Mitteilung mit Lösungen vorbereitet werden).
  - Schrittweise Rückkehr zum normalen Betriebsmodus.

## 6.6. Nach dem Rollout – Betrieb und kontinuierliche Verbesserung

Die Einführung von MFA ist kein einmaliges Ereignis, sondern ein neuer Betriebszustand der Sicherheitsinfrastruktur. Nach Abschluss des Implementierungsprojekts sollte der Fokus auf dem laufenden Betrieb des Systems sowie der kontinuierlichen Verbesserung der MFA-Richtlinien und des

Authentifizierungsprozesses liegen. Im Folgenden finden Sie die wichtigsten Punkte, die in der Betriebsphase zu beachten sind:

- **Überwachung der Sicherheit und Auswertung von Erkenntnissen.** Es ist wichtig, die Anmeldeprotokolle regelmäßig im Hinblick auf Sicherheitsvorfälle zu überprüfen. Achten Sie dabei auf ungewöhnliche Anmeldezeiten (z. B. um 3 Uhr morgens, wenn normalerweise niemand arbeitet) sowie auf wiederholte fehlgeschlagene Anmeldeversuche (z. B. Dutzende abgelehnter Versuche für einen einzigen Benutzer). Zudem sollte analysiert werden, wie effektiv MFA ist – beispielsweise ob seit der Einführung die Anzahl der kontobezogenen Sicherheitsvorfälle gesunken ist.



- **Rotation von Geräten und Updates.** Es ist wichtig zu berücksichtigen, dass die Arbeitsumgebung dynamisch ist: Mitarbeitende wechseln ihre Telefone, neue Teammitglieder kommen hinzu und andere verlassen das Unternehmen.
    - Es sollte ein Prozess für die Aktivierung von MFA für neue Mitarbeitende eingerichtet werden. Zum Beispiel könnten neue Mitarbeitende am ersten Arbeitstag ein Starterpaket erhalten: „*Dies ist Ihr Firmencomputer und hier ist der Link zur MFA-Konfiguration für Ihr Konto. Bitte führen Sie dies sofort durch.*“.
    - Es sollte ebenfalls ein klar definierter Prozess vorliegen, um MFA für Mitarbeitende zu deaktivieren, die das Unternehmen verlassen.
    - Es ist sinnvoll, Mitarbeitende anzuweisen, die MFA-Client-Anwendungen regelmäßig zu aktualisieren, sofern solche existieren. Falls der MFA-Anbieter eine eigene mobile App anbietet, sollte die regelmäßige Aktualisierung empfohlen oder eine automatische Aktualisierung aktiviert werden.
    - Auch Server und lokal bereitgestellte MFA-Dienste sollten aktualisiert werden, sobald neue Versionen verfügbar sind. Neue Produktversionen enthalten häufig

sicherheitsrelevante Verbesserungen und neue Funktionen, weshalb regelmäßige Updates sehr wichtig sind.

- **Überprüfung von Ausnahmen und Sonderkonten.** Wenn es Konten gibt, die nicht MFA-pflichtig sind (zum Beispiel Notfall- oder Servicekonten), muss sichergestellt werden, dass diese durch andere Methoden gut abgesichert und regelmäßig geprüft werden. Die Passwörter für solche Konten sollten besonders stark sein und in einem sicheren Passwortmanager gespeichert werden. Es sollte überwacht werden, ob diese Konten tatsächlich nur in Ausnahmefällen genutzt werden, und es sollte regelmäßig bewertet werden, ob MFA nicht doch für diese Konten aktiviert werden sollte.

- **Erweiterung auf weitere Gruppen und Benutzer.** Es kann sinnvoll sein, nach der grundlegenden Einführung für die Mitarbeitenden auch Kunden oder externe Partner, die Zugriff auf bestimmte Unternehmensressourcen haben, in die MFA einzubeziehen. Viele MFA-Lösungen ermöglichen dies, zum Beispiel durch Integration mit einem Kundenportal. Wenn es in einem bestimmten Kontext sinnvoll ist (zum Beispiel zum Schutz des Zugangs von Auftragnehmern zu einem Bestellsystem), sollte die Nutzung der bestehenden MFA-Infrastruktur in Betracht gezogen werden. Dadurch lässt sich ein zusätzlicher Nutzen aus der bereits getätigten Investition erzielen.

Zusammenfassend lässt sich sagen, dass die Einführung von MFA ein fortlaufender Prozess ist. Nach der Projektphase folgt die operative Phase, in der MFA ähnlich wie jedes andere wichtige Sicherheitssystem verwaltet werden muss. Die gute Nachricht ist, dass der Betrieb von MFA nach der intensiven Einführungsphase nicht mehr viel Zeitaufwand erfordert. Dennoch sollte man sich nicht zurücklehnen. Es ist wichtig, die Wirksamkeit der Lösung zu überwachen und ihre Zuverlässigkeit sicherzustellen. Lösungen wie Rublon MFA ermöglichen es, Anmeldevorgänge zu überwachen, die Effektivität der verwendeten MFA-Methoden zu analysieren und die Aktivität der Benutzer zu verfolgen, was den Betrieb der Lösung in der Nachbereitungsphase erleichtert.

## 6.7. Praktische Checkliste: Worauf nach der Einführung von MFA zu achten ist

Nachfolgend finden Sie eine kurze Checkliste der wichtigsten Aspekte, auf die Sie nach der Einführung von MFA in der Organisation achten sollten:

- **Überwachung von MFA-Vorfällen:**
  - Sie sollten regelmäßig die Protokolle analysieren und auf verdächtige Ereignisse achten, zum Beispiel viele falsche Codes, abgelehnte Push-Benachrichtigungen oder Anmeldungen aus anderen Ländern.

- **Überprüfung der Zugriffsrichtlinien:**
  - Sie sollten die MFA-Richtlinien regelmäßig überprüfen und bei Bedarf anpassen.
  - Es kann sinnvoll sein, neue Authentifizierungsmethoden zu aktivieren oder ältere Methoden zu entfernen, wenn diese als nicht mehr ausreichend sicher eingestuft werden.

- **Systemaktualisierungen:**
  - Sie sollten regelmäßige, geplante Aktualisierungen der Server und Dienste von MFA sowie der Client-Anwendungen einplanen.
  - Es ist empfehlenswert, diese Aktualisierungen vorab in einer sicheren Testumgebung durchzuführen, bevor sie in der produktiven Umgebung eingesetzt werden.

- **Identitätsverwaltung:**
  - Sie sollten Verfahren erstellen, um MFA für neue Mitarbeitende zu aktivieren sowie ausscheidende Mitarbeitende aus der MFA-Plattform zu entfernen.
  - Falls es noch Konten ohne MFA gibt, sind regelmäßige Audits erforderlich und die endgültige Aktivierung der Multi Faktor Authentifizierung auf diesen Konten sollte erfolgen, sofern möglich.

- **Privilegierte und Notfallkonten:**
  - Privilegierte Konten und Administratorkonten sollten besonders stark durch Multi-Faktor-Authentifizierung abgesichert werden. Bevorzugt werden MFA-Methoden, die phishingresistent sind.
  - Notfallkonten müssen besonders stark geschützt und regelmäßig überprüft werden.

- **Auffrischungsschulungen:** Sie sollten Informationen über Multi Faktor Authentifizierung in regelmäßige Sicherheitsschulungen für Mitarbeitende einbeziehen. Während dieser Schulungen sollten Sie über die sichere Nutzung von MFA informieren und über mögliche Angriffsarten auf dieses Sicherheitsverfahren aufklären, zum Beispiel über Social Engineering.

- **Notfallplan:** Sie sollten einen funktionierenden Notfallplan haben, zum Beispiel einen halbjährlich getesteten Plan, für den Fall einer vorübergehenden Nichtverfügbarkeit des MFA-Systems. Notfallkonten sowie alternative Zugriffskonfigurationen müssen in solchen Situationen verfügbar sein und das Personal muss wissen, wie diese zu nutzen sind. Nach Behebung der Störung müssen alle Mitarbeitenden wieder wie gewohnt MFA verwenden.

# 7. Sicherstellung der Geschäftskontinuität bei der Nutzung von MFA

Die Einführung der Multi Faktor Authentifizierung erhöht das Sicherheitsniveau in der Organisation erheblich, fügt jedoch gleichzeitig eine neue technologische Abhängigkeit hinzu. Was passiert, wenn das MFA-System ausfällt oder wenn ein Nutzer alle seine Authentifizierungsmethoden verliert? Die Sicherstellung der Geschäftskontinuität bedeutet, dass Sie auf solche Szenarien vorbereitet sind, damit eine Unterbrechung der MFA-Verfügbarkeit den Betrieb der Organisation nicht stoppt. Im Folgenden finden Sie vorbeugende Maßnahmen und bewährte Verfahren, die Ihnen ermöglichen, MFA zu nutzen, ohne Angst vor Arbeitsausfällen oder Unterbrechungen zu haben.

**Erfahren Sie, wie Sie einen unterbrechungsfreien Betrieb der Multi-Faktor-Authentifizierung sicherstellen können, mithilfe des Rublon-Leitfadens zur Gewährleistung der Geschäftskontinuität.**

## 7.1. Redundanz und hohe Verfügbarkeit des MFA-Systems

Wenn die MFA-Lösung lokale Komponenten umfasst (engl. on-premise), sollte für deren hohe Verfügbarkeit (high availability) gesorgt werden. Dies kann durch die Konfiguration eines Clusters im Active-Passive- oder Active-Active-Modus, durch die Platzierung von Servern an zwei verschiedenen Standorten sowie durch die Sicherstellung aktueller Backups der Datenbank erreicht werden.

Es ist außerdem wichtig, die Failover-Mechanismen gründlich zu testen, um sicherzustellen, dass sie im Störungsfall zuverlässig funktionieren. Beispielsweise sollte geprüft werden, ob im Fall eines Ausfalls des Haupt-Proxy-Servers, der MFA hinzufügt, ein redundanter Server sofort die Anfragen übernimmt, sodass die Benutzer keine Unterbrechung bemerken.

Wenn der MFA-Anbieter seine Dienste in der Cloud bereitstellt, sollten die Service-Level-Agreement-(SLA-)Bestimmungen sowie die Architektur der Lösung überprüft werden.

Es ist entscheidend, dass ein einzelner Ausfall nicht den gesamten Anmeldeprozess im Unternehmen lahmlegt. Daher sollte die MFA-Lösung auf ihre Widerstandsfähigkeit getestet werden, zum Beispiel:

- Was passiert, wenn die Internetverbindung ausfällt? Können sich die Mitarbeitenden weiterhin an ihren Geräten anmelden?
- Funktionieren die Failover-Mechanismen wie vorgesehen und lassen sie die Anmeldung entweder zu oder lehnen sie korrekt ab?
- Sind die Notfallcodes verfügbar, funktionieren sie ordnungsgemäß und werden sie nach der Nutzung ersetzt?

## 7.2. Eliminierung einzelner Ausfallpunkte

Es sollte sichergestellt werden, dass die Benutzer alternative MFA-Methoden zur Verfügung haben, falls es zu Problemen mit der Hauptmethode kommt. Wenn die Mitarbeiter einer Organisation beispielsweise hauptsächlich Push-Benachrichtigungen in der mobilen App verwenden, muss gewährleistet sein, dass sie im Bedarfsfall auch eine andere Authentifizierungsmethode nutzen können oder einen Notfallcode erhalten.

Wenn Mitarbeitende Sicherheitsschlüssel (FIDO-Schlüssel) verwenden, empfiehlt es sich, dass sie einen zweiten Ersatzschlüssel besitzen. Dies ist besonders wichtig, wenn der Zugang zu kritischen Ressourcen ausschließlich mit FIDO-Sicherheitsschlüsseln geschützt werden kann. In diesem Fall sollte die Organisation jedem Benutzer zwei Schlüssel ausgeben: einen für den täglichen Gebrauch und einen zweiten, der an einem sicheren Ort aufbewahrt wird, falls der erste verloren geht.

Die interne Sicherheitsrichtlinie der Organisation sollte dazu ermutigen, mindestens zwei verschiedene MFA-Methoden zum Benutzerkonto hinzuzufügen.

## 7.3. Verfahren zur Wiederherstellung des Zugangs

Es besteht stets das Risiko, dass ein Benutzer den Zugang zu seinem Konto verliert. Daher muss ein formaler Prozess existieren, der es ermöglicht, die Identität des Benutzers sicher zu überprüfen und den Zugang wiederherzustellen. Solche Vorfälle sollten ordnungsgemäß dokumentiert und von einer

vorgesetzten Person bestätigt werden, um Missbrauch zu verhindern. Ein typisches Verfahren zur Wiederherstellung des Zugangs sollte wie folgt aussehen:

1. Der Benutzer nimmt Kontakt mit dem externen technischen Support auf.
2. Der Support-Mitarbeiter überprüft die Identität des Benutzers anhand mehrerer spezifischer Fragen. Diese müssen ausreichend präzise sein, um eine eindeutige Identifikation zu gewährleisten und eine unbefugte Person am Zugang zu hindern.
3. Nach erfolgreicher Verifizierung generiert der Support-Mitarbeiter einen einmaligen Notfall-Code oder sendet einen Link mit der Möglichkeit, ein neues Authentifizierungsgerät für MFA zu konfigurieren.

**Erfahren Sie, wie Sie Notfall-Zugangscodes (Bypass-Codes) in Rublon MFA verwenden können.**

## 7.4. Notfallkonten und Notfallzugänge für Administratoren

Je nach Infrastruktur der Organisation können Notfallzugangskonten erforderlich sein, um die Kontinuität des Betriebs kritischer Systeme sicherzustellen. Diese Konten können für Situationen dienen, in denen Administratoren sich nicht anmelden können, z. B. wenn ein Ausfall des MFA-Systems auftritt.

Anstatt vollständig auf MFA zu verzichten, kann MFA im Offline-Modus verwendet werden, etwa mithilfe von Einmalcodes, die durch die mobile App generiert werden. Die Passwörter solcher Konten müssen außergewöhnlich stark und entsprechend geschützt sein (z. B. in versiegelten Umschlägen im Vorstandstresor oder in einem sicheren Passworttresor mit Zugriff nur für autorisierte Personen).

In großen Umgebungen lohnt es sich, einen Bastion-Host (engl. bastion host oder jump host) einzurichten, also ein System, das vollständig vom Internet getrennt ist und über ein VPN erreichbar ist und eigene Notfallkonten mit MFA im Offline-Modus hat. Dieser Ansatz ermöglicht es, das Prinzip „kritischster Zugriff = stärkstes MFA“ einzuhalten, ohne das Team im Fall einer Nichtverfügbarkeit der Multi-Faktor-Authentifizierung vom Zugriff abzuschneiden.

Das Szenario für die Nutzung von Notfallkonten sollte regelmäßig getestet werden. Wenn das MFA-System nicht funktioniert, verwendet der Administrator ein Notfallkonto, meldet sich an einer dedizierten PAW-Station an und diagnostiziert das Problem. Jeder solcher Vorfall sollte im SIEM-System dokumentiert werden, gemäß NIST AC-2(2).

## 7.5. Temporäre Ausschlüsse und „Fail-open“-Mechanismen

Es lohnt sich zu analysieren, ob es Situationen gibt, in denen der Zugriff nicht ausschließlich von MFA abhängig sein darf. Beispiele sind medizinische Systeme, die 24/7 laufen, bei denen ein Arzt sofortigen

Zugriff auf das System benötigt. Was tun, wenn der Benutzer den Authentifizierungscode auf sein Telefon nicht erhält?

In solchen Fällen kann eine Anmeldung mit nur einem Faktor in Ausnahmefällen (sog. fail-open) in Erwägung gezogen werden. Dies ist jedoch eine sehr heikle Angelegenheit, da der Missbrauch eines solchen Mechanismus ein erhebliches Sicherheitsrisiko darstellen kann.

Alternative Ansätze sind Offline-Lösungen, zum Beispiel Hardware-Tokens oder mobile Anwendungen, die OTP-Codes ohne Internetzugang generieren. In einer Notsituation, zum Beispiel bei einem Telefon- oder Internetausfall, kann der Mitarbeiter auch einen zuvor ausgegebenen Umschlag mit Notfallcodes verwenden.

Wichtig ist, dass Notfallverfahren klar definiert sind und nur autorisierten Personen bekannt sind. Gleichzeitig muss dafür gesorgt werden, dass Notfallcodes angemessen geschützt werden, damit sie nicht zu einer öffentlich zugänglichen Schwachstelle im System werden.

**Erfahren Sie, wie der Notfallmodus (Fail Mode) in Rublon MFA Connectors funktioniert.**

## 7.6. Regelmäßige DR-Tests (Disaster Recovery)

Die Rublon MFA Plattform sollte in die Business-Continuity- und Disaster-Recovery-Pläne der Organisation aufgenommen werden. Wenn DR-Tests durchgeführt werden, zum Beispiel die Simulation eines Data-Center-Ausfalls, muss das Szenario berücksichtigt werden, in dem der MFA-Authentifizierungsserver nicht verfügbar ist. Es sollte geschätzt werden, wie viel Zeit die Wiederherstellung benötigt und ob die Mitarbeiter währenddessen im Notfallmodus arbeiten können. Notfallverfahren sollten ebenfalls getestet werden. Zum Beispiel kann einmal pro Quartal ein ausgewählter Administrator gebeten werden, zu prüfen, ob er sich gemäß Dokumentation über ein Notfallkonto anmelden kann.

## 7.7. Überwachung der Verfügbarkeit von MFA-Diensten

Es ist sinnvoll, die Status-Seite des MFA-Anbieters zu abonnieren (Status Page). Dadurch kann eindeutig festgestellt werden, ob Login-Probleme bei den Mitarbeitern vom Anbieter verursacht werden. Status-Seiten enthalten oft eine Übersicht über die gesamte Infrastruktur des MFA-Dienstes und deren einzelne Komponenten. Dank solcher Benachrichtigungen ist es viel einfacher, einen Ausfall des GSM-Betreibers in einer Region oder eine Störung beim MFA-Dienstanbieter zu identifizieren, was erklärt, warum SMS-Codes oder Einmalcodes einige Mitarbeiter nicht erreichen. Mit diesem Wissen kann man schnell die Standard-Authentifizierungsmethoden anpassen oder die Mitarbeiter über die Notwendigkeit informieren, auf eine andere Methode umzusteigen.

## 7.8. Sicherheit von Schlüsseln und physischen Token

Wenn in der Organisation Sicherheitsschlüssel oder Smartcards verwendet werden, muss eine Richtlinie für deren Austausch und Meldung von Verlusten definiert werden. Mitarbeiter müssen wissen, dass der Verlust eines FIDO-Schlüssels vergleichbar mit dem Verlust eines Haustürschlüssels ist und sofort gemeldet werden muss, auch wenn der Schlüssel möglicherweise nicht direkt sensibel ist. Für Mitarbeiter mit kritischem Zugriff ist es sinnvoll, Ersatzschlüssel vorzuhalten, damit neue Schlüssel im Bedarfsfall schnell ausgegeben werden können, auch wenn dies mehr Aufwand bedeutet. Wesentlich ist die Ausgabe zweier Schlüssel: eines Hauptschlüssels und eines Ersatzschlüssels. Zudem sollte dokumentiert werden, welche Schlüssel ausgegeben wurden. Falls Token eine begrenzte Lebensdauer haben, zum Beispiel wenn Zertifikate auf Karten alle zwei Jahre ablaufen, sollten rechtzeitige Erinnerungen für deren Erneuerung eingerichtet werden.

## 7.9. Praktische Checkliste: Sicherstellung der Geschäftskontinuität

Nachfolgend finden Sie eine kurze Checkliste zu den wichtigsten Aspekten der Sicherstellung der Geschäftskontinuität Ihrer Organisation beim Einsatz von MFA.

- **Redundanz der MFA-Plattform:**
  - Konfigurieren Sie einen aktiv-passiv oder aktiv-aktiv Cluster sowie Instanzen in zwei getrennten Standorten.
  - Testen Sie das Failover. Prüfen Sie, ob der Ersatzserver den Datenverkehr ohne Unterbrechung für die Benutzer übernimmt.
  - Überprüfen Sie den SLA und die Architektur Ihres Cloud-Anbieters.
  - Stellen Sie sicher, dass die lokale Anmeldung auch dann funktioniert, wenn die Internetverbindung ausfällt.

- **Eliminierung einzelner Ausfallpunkte:**
  - Erzwingen Sie mindestens zwei unterschiedliche MFA-Methoden pro Benutzerkonto.
  - Stellen Sie Notfallcodes oder alternative Authentifizierungsmethoden für dringende Fälle bereit.

- **Verfahren zur Wiederherstellung des Zugangs:**
  - Definieren Sie die Schritte zur Identitätsüberprüfung, zum Beispiel Sicherheitsfragen oder Kontaktaufnahme mit der vorgesetzten Person.
  - Dokumentieren Sie die Generierung eines Einmalpassworts oder eines Links zur erneuten Registrierung von MFA.
  - Protokollieren Sie jeden Vorfall und lassen Sie ihn von einer vorgesetzten Person freigeben.

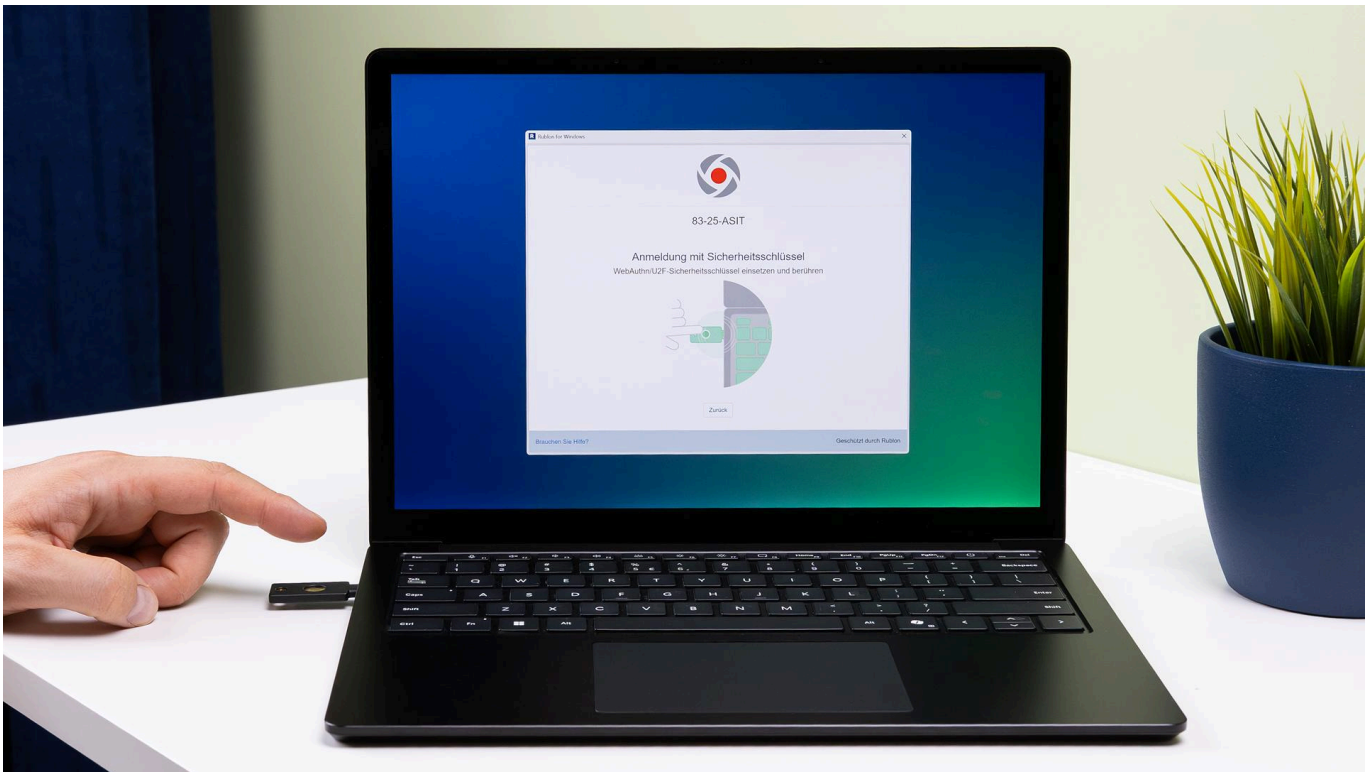
- **Notfallkonten und Notfallwege für Administratoren:**
  - Halten Sie ein bis zwei sogenannte Break-Glass-Konten bereit, bestehend aus Passwort und offline nutzbarem MFA.
  - Bewahren Sie die Passwörter in einem Tresor auf, der nur für die Geschäftsführung oder den CISO zugänglich ist.
  - In großen Umgebungen sollte ein Bastion-Host hinter VPN mit eigenen Notfallkonten eingerichtet werden.
  - Testen Sie die Notfallanmeldung regelmäßig und ändern Sie das Passwort nach jeder Nutzung. Dokumentieren Sie den Vorfall im SIEM.

- **Zeitweilige Ausnahmen und der Fail-Open-Mechanismus:**
  - Bereiten Sie MFA-Methoden vor, die offline funktionieren, oder nutzen Sie versiegelte Umschläge mit OTP-Codes.
  - Beschränken Sie das Notfallverfahren ausschließlich auf berechtigte Personen und dokumentieren Sie jede Nutzung.

- **Regelmäßige DR-Tests:**
  - Berücksichtigen Sie den MFA-Dienst in den Business-Continuity- und Disaster-Recovery-Plänen.
  - Simulieren Sie mindestens einmal pro Quartal die Nichtverfügbarkeit von MFA.
  - Messen Sie die Wiederanlaufzeit des MFA-Dienstes (RTO) sowie die Bereitschaft der Mitarbeitenden, im Notfallbetrieb zu arbeiten.

- **Überwachung des Zustands von MFA-Diensten:**
  - Abonnieren Sie die Statusseite Ihres MFA-Anbieters und aktivieren Sie Benachrichtigungen zu Änderungen im Dienststatus.
  - Konfigurieren Sie Alarme für kritische Komponenten.

- **Sicherheit physischer Schlüssel und Token:**
  - Führen Sie ein Register aller ausgegebenen Geräte und verlangen Sie die unverzügliche Meldung von Verlusten.
  - Geben Sie zwei Schlüssel pro Person aus (Hauptschlüssel und Ersatzschlüssel).
  - Richten Sie Erinnerungen zur rechtzeitigen Erneuerung von Zertifikaten oder Smartcards vor deren Ablauf ein.




# 8. Anhang 1: Methoden der MFA-Authentifizierung

Bei der Auswahl der Authentifizierungsmethoden in einer Organisation sollte man sich nach dem Grundsatz der Risikoadäquanz richten. Für die Mehrheit der Mitarbeitenden werden mobile Anwendungen (Codes oder Push) eine akzeptable Methode darstellen, während für besonders gefährdete Konten bereits der Einsatz von FIDO-Hardware-Schlüsseln erforderlich ist. Es sollten keine sicherheitskritischen Zugriffe über leicht zu kompromittierende Methoden wie SMS oder E-Mail abgesichert werden. Solche Methoden können zwar als Notfalloption dienen, sollten jedoch nicht die Grundlage der Authentifizierung bilden.

In der internen Dokumentation sollten alle Benutzergruppen und Ressourcen mit den ihnen zugewiesenen, erforderlichen MFA-Methoden klar beschrieben werden. Ein solcher Leitfaden ermöglicht die Standardisierung der Authentifizierungsverfahren und stellt Konsistenz sowie die Einhaltung der Sicherheitsrichtlinien der Organisation sicher.

| MFA-Methode | Widerstandsfähigkeit gegenüber Cyberangriffen | Wichtigste Hinweise zur Sicherheit und Anwendung |
|---|---|---|
| **FIDO2-Hardware-Schlüssel** | **Sehr hoch** – kryptografisch an die Domain gebunden, resistent gegen Phishing und „Man-in-the-Middle"-Angriffe. | Empfohlen für privilegierte Konten sowie für kritische Systeme. Es sollten immer zwei Schlüssel ausgegeben werden (Hauptschlüssel + Ersatzschlüssel), und deren Ausgabe und Nutzung ist zu dokumentieren. |
| **Karte mit PKI (Smartcard / PKI)** | **Hoch** – der private Schlüssel ist durch die Karte und einen PIN geschützt und verlässt das Gerät nie. | Erfordert eine vollständige PKI-Infrastruktur und Kartenleser; weit verbreitet in Behörden (PIV-Karten) und regulierten Organisationen. |
| **Passkey** | **Hoch** – resistent gegen Phishing, die Verifizierung erfolgt lokal (Biometrie / PIN). | Benutzerfreundlich; bei synchronisierten Passkeys werden private Schlüssel in der Cloud gespeichert – dies erfordert passende Richtlinien der Apple/Google/Microsoft-Ökosysteme oder Einstellungen des Passwortmanagers. |
| **Mobile App – Push-Benachrichtigung** | **Mittel oder Hoch** – bei Nutzung von Number Matching reduziert es Push Bombing und versehentliche Bestätigungen und erhöht damit die Sicherheit. | Guter Kompromiss zwischen Benutzerfreundlichkeit und Sicherheit; erfordert eine Internetverbindung auf dem Telefon; dennoch anfällig für komplexe Phishing-Szenarien. |
| **YubiKey OTP** | **Mittel** –der Code wird automatisch durch Drücken des Schlüssels eingetippt, bleibt aber phishinganfällig (Angreifer kann ihn sofort verwenden). | Benutzerfreundlich, da kein Abtippen notwendig ist, jedoch anfällig für Phishing. Wenn bereits Hardware-Schlüssel angeschafft wurden, empfiehlt sich statt YubiKey OTP ein phishingresistenter FIDO2-Modus. |
| **Mobile App – TOTP-Code** | **Mittel** – der Code kann per Phishing abgefangen werden, erfordert jedoch meist Zugriff auf das Gerät oder Malware. | Funktioniert offline; erfordert manuelles Eintippen (potenziell Shoulder Surfing). Nur dort einsetzen, wo sicherere Methoden nicht möglich sind. |

| | | |
|---|---|---|
| **Hardware-OTP-Token** | **Mittel** – einmaliger Code, aber ebenfalls phishinganfällig. | Unabhängig vom Telefon; erfordert organisatorischen Aufwand (Ausgabe, Batterien). Häufig ersetzt durch TOTP-Apps oder FIDO-Schlüssel. |
| **Mobile App – QR-Code** | **Mittel** – einmaliger Code, kann jedoch abgefangen werden, wenn der Bildschirm öffentlich sichtbar ist. | Der Code sollte sofort nach der Verwendung ablaufen. |
| **SMS-OTP / Telefonanruf** | **Niedrig** – anfällig für Phishing, SIM-Swap und SS7-Angriffe. | Nur für Notfälle oder für Benutzer ohne Smartphone geeignet; mittelfristig Migration auf stärkere Methoden einplanen. |
| **E-Mail-OTP** | **Niedrig** – Schutz hängt vollständig von der Sicherheit des E-Mail-Kontos ab. | Nur als Notfallmethode verwenden; auch die E-Mail muss idealerweise selbst durch MFA geschützt werden. |
| **Backup- / Notfallcodes** | **Hängt davon ab, wie sie gespeichert werden** – Papier oder Datei kann gestohlen werden. | Nur für eine begrenzte Anzahl von Anwendungen generieren und dem Benutzer sicher übermitteln; offline und geschützt aufbewahren. |

# 9. Anhang 2: Regulatorische Anforderungen an MFA

Die folgende Tabelle enthält die wichtigsten Rechtsakte und Richtlinien, die öffentlichen oder beaufsichtigten Einrichtungen ausdrücklich die Pflicht auferlegen, Multi-Faktor-Authentifizierung (MFA) oder „starke Authentifizierung“ anzuwenden.

Andere Vorschriften, zum Beispiel die DSGVO oder die Verordnung über den Nationalen Interoperabilitätsrahmen, sprechen allgemein von „angemessenen technischen Maßnahmen“ oder von der „Umsetzung einer Informationssicherheitsrichtlinie“. In der Praxis erkennen Aufsichtsbehörden immer häufiger MFA als eine angemessene Maßnahme zur Abdeckung der meisten Risiken an, die mit privilegiertem oder remote Zugriff verbunden sind.

| Jurisdiktion / Sektor | Rechtsakt / Dokument | Artikel / Paragraph | Umfang der MFA-Anforderung |
|---|---|---|---|
| **EU – wesentliche und wichtige Einrichtungen** | Richtlinie (NIS2) 2022/2555 | Art. 21 Abs. 2 Buchst. d, i, j | MFA unterstützt die Sicherheit der Lieferkette, der Personalressourcen und der Zugangskontrolle. Sie ist erforderlich, um Kommunikationssysteme und Notfallsysteme dort zu schützen, wo dies anwendbar ist. |
| **EU – Finanzsektor** | Verordnung (DORA) 2022/2554 | Art. 9 Abs. 3 Buchst. b–c; Art. 4 Abs. c–d | MFA unterstützt die Umsetzung der ICT-Sicherheitsrichtlinien durch Minimierung des Risikos unbefugten Zugriffs, Schutz der Vertraulichkeit und Integrität von Daten und Kontrolle des Zugangs zu ICT-Ressourcen. Darüber hinaus stellt sie eine direkte Anforderung dar, da ein „starker Authentifizierungsmechanismus“ gemäß den Standards verlangt wird. |
| **EU – Zahlungsdienste** | PSD2 (2015/2366), RTS 2018/389 | PSD2 (2015/2366) Art. 97, RTS 2018/389 Art. 4–9 | Starke Kundenauthentifizierung (SCA) ist erforderlich beim Zugriff auf ein Online-Konto, bei der Einleitung elektronischer Zahlungen sowie bei jeder Remote-Aktion mit Betrugsrisiko. Sie muss auf mindestens zwei unabhängigen Faktoren aus den Kategorien Wissen, Besitz oder Inhärenz basieren. |

**Beispiele für MFA-Anforderungen außerhalb der EU**

- **USA – NIST SP 800-53 Rev. 5**
  Kontrolle IA-2(1)(2): MFA für privilegierte und nicht privilegierte Konten. IA-2 legt technische Standards für MFA in föderalen Systemen fest.

- **USA – Executive Order 14028**
  § 3(d) verpflichtet alle Bundesbehörden zur Einführung von MFA.

- **USA – OMB M-22-09 „Federal Zero Trust Strategy"**
  Verlangt phishingresistente MFA für Mitarbeiter und Auftragnehmer sowie die Konsolidierung von Identitätssystemen.

- **USA – NIST SP 800-171 Rev. 3**
  Wymaga MFA dla wszystkich kont uprzywilejowanych *i* zwykłych w systemach przetwarzających CUI.

**Warum ist das wichtig?**

Die dynamische Entwicklung der Regulierung in den USA zeigt die Richtung auf: weg von „beliebiger" MFA hin zu verpflichtenden, phishingresistenten Methoden wie FIDO2 oder PIV. Eine ähnliche Entwicklung ist auch in der EU absehbar. Bereits jetzt enthalten die neuesten Leitlinien der ENISA im Dokument „NIS2 Technical Implementation Guidance" entsprechende Empfehlungen. Die öffentliche Verwaltung, die MFA-Projekte vorbereitet, sollte daher von Anfang an Mechanismen einplanen, die dem FIDO2-Standard entsprechen, um spätere kostspielige Änderungen zu vermeiden.

# 10. Anhang 3: Glossar

- **Active Directory (AD)** — Microsoft-Verzeichnisdienst zur Authentifizierung, Autorisierung und zentralen Verwaltung von Benutzern, Computern und Ressourcen in einer Windows-Domänenumgebung.

- **Active Directory Federation Services (AD FS)** — ein von Microsoft entwickelter standardbasierter Dienst, der föderiertes Identitäts- und Zugriffsmanagement ermöglicht und Identitätsinformationen zwischen vertrauenswürdigen Partnern sicher austauscht. AD FS erweitert Single Sign-On (SSO) über Sicherheits- und Unternehmensgrenzen hinweg, sodass Benutzer nahtlos auf geschützte Anwendungen zugreifen können.

- **Authenticator Assurance Level (AAL)** — das gemäß der NIST-Klassifikation definierte Niveau der Authentisierungsstärke, das das Vertrauen in einen Authentifizierungsmechanismus beschreibt. AAL1 entspricht einem niedrigen Sicherheitsniveau (z. B. Passwort), AAL2 einem mittleren (z. B. Passwort + TOTP) und AAL3 einem hohen Niveau (z. B. Passwort + FIDO2-Hardware).

- **Geräteregistrierung** — Der Prozess des Hinzufügens eines Benutzergeräts zur MFA-Plattform, um eine Authentifizierungsmethode wie eine mobile App oder einen FIDO-Schlüssel zu konfigurieren. Dies kann vom Benutzer selbst durchgeführt oder zentral von einem Administrator verwaltet werden.

- **DORA (Digital Operational Resilience Act)** — Die EU-Verordnung 2022/2554 zur operativen Resilienz von Finanzinstituten und IKT-Dienstleistern schreibt die Anwendung starker Authentifizierungsmethoden (z. B. Multi-Faktor-Authentifizierung), digitales Risikomanagement, Resilienztests und die Meldung von Vorfällen vor. Sie gilt unter anderem für Banken, Versicherungen, Fintech-Unternehmen und Cloud-Dienstleister.

- **ENISA (Agentur der Europäischen Union für Cybersicherheit)** — Die Agentur der Europäischen Union für Cybersicherheit (Euro-Agentur für Cybersicherheit) veröffentlicht Leitlinien, Best Practices und Berichte zur IT-Systemsicherheit, darunter Empfehlungen zu Multi-Faktor-Authentifizierung (MFA), digitaler Identität, Vorfallmanagement und der Umsetzung der NIS2-Richtlinie. Obwohl sie keine formale Auslegungsfunktion besitzt, gelten ihre Dokumente weithin als verlässliche Quelle für technische Unterstützung bei EU-Vorschriften.

- **Entra ID (ehemals Azure AD)** — Der Cloud-Verzeichnisdienst von Microsoft zur Verwaltung von Benutzeridentitäten, Zugriffsrechten und Authentifizierung in Hybrid- und Cloud-Umgebungen. Unterstützt Multi-Faktor-Authentifizierung (MFA), Single Sign-On (SSO) und verschiedene Anmeldemethoden.

- **Fail-open** — ein Zustand oder Mechanismus, bei dem ein System im Fehlerfall (z. B. bei Nichtverfügbarkeit der MFA) weiterhin Zugang gewährt, anstatt die Authentifizierung zu blockieren. Diese Konfiguration wird nur in Ausnahmefällen eingesetzt und erfordert klare Kontrollprozesse und Sicherheitsrichtlinien.

- **FIDO2** — Ein offener Standard für moderne, phishingresistente Authentifizierung, entwickelt von der FIDO Alliance. Er ermöglicht die Anmeldung mittels Sicherheitsschlüsseln, integrierter Biometrie oder Passkeys.

- **Hochverfügbarkeit (HA)** — die Architektur von IT-Systemen, die deren ununterbrochenen Betrieb trotz des Ausfalls einzelner Komponenten gewährleistet.

- **Notfallkonto**— Ein dediziertes Notfallkonto mit privilegierten Zugriffsrechten, das ausschließlich für kritische Situationen wie den Ausfall eines Cloud-MFA-Systems vorgesehen ist. Solche Konten sollten mit Offline-MFA geschützt und regelmäßig überwacht werden.

- **LDAP (Lightweight Directory Access Protocol)** — ein leistungsoptimiertes, leichtgewichtiges Netzwerkprotokoll zum Abfragen und Ändern von Daten in Verzeichnisdiensten wie Active Directory, OpenLDAP oder anderen LDAP-kompatiblen Systemen. Es ermöglicht hierarchischen Zugriff auf Benutzerkonten, Gruppen, Geräte und weitere Ressourcen.

- **Multi-Faktor-Authentifizierung (MFA)** — Eine Form der Identitätsprüfung, bei der ein Nutzer mindestens zwei verschiedene Authentifizierungsfaktoren angeben muss, um festzustellen, ob er tatsächlich derjenige ist, für den er sich ausgibt. Zu diesen Authentifizierungsfaktoren gehören Wissen (z. B. ein Passwort oder eine PIN), Besitz (z. B. ein Sicherheitsschlüssel oder ein Smartphone) und charakteristische Merkmale (z. B. ein Fingerabdruck oder ein Gesicht).

- **NIS2 (Richtlinie 2 über Netz- und Informationssicherheit)** — EU-Richtlinie (2022/2555) zur Cybersicherheit von Netzen und Informationssystemen. Sie erweitert den Kreis derjenigen, die den Sicherheitsverpflichtungen unterliegen (einschließlich öffentlicher Verwaltung, Gesundheitswesen, Energie, Bankwesen, digitale Technologien) und erhöht die Anforderungen an das Risikomanagement, einschließlich der Verwendung von MFA, Identitätsmanagement und Vorfallsüberwachung.
und Geschäftskontinuität.

- **Number matching (Nummernabgleich)** — ein Sicherheitsmechanismus für Push-Authentifizierungen, bei dem der Benutzer die auf dem Anmeldebildschirm angezeigte Zahl in der mobilen MFA-App eingeben muss. Dieser Mechanismus schützt vor Push-Bombing-Attacken und versehentlichen Genehmigungen.

- **Phishing-Resistenz** — ein Merkmal von Authentifizierungsmethoden, die so ausgelegt sind, dass sie durch Phishing-Angriffe nicht kompromittiert werden können. Ziel ist es, zu verhindern, dass Benutzer durch gefälschte Login-Seiten oder manipulierte Anmeldeversuche zur Preisgabe von Zugangsdaten verleitet werden.

- **Einmalpasswort (OTP)** — Ein Einmalpasswort zur Bestätigung der Identität eines Benutzers. Wird meist als zweiter Faktor bei der Multi-Faktor-Authentifizierung verwendet.

- **Outlook Web App (OWA)** — eine Komponente des Microsoft Exchange Servers, die den Zugriff auf E-Mails über einen Webbrowser ermöglicht. Aufgrund des Fernzugriffs wird sie oft als eine der ersten Ressourcen für die Implementierung von MFA genannt.

- **Passkey** — eine moderne Authentifizierungsmethode, die es Benutzern ermöglicht, sich ohne Passwörter anzumelden, indem sie ein Paar kryptografischer Schlüssel verwendet, die dem FIDO2-Standard entsprechen.

- **Phishing** — Phishing ist eine Angriffsmethode, bei der sich jemand als vertrauenswürdige Person ausgibt (z. B. durch gefälschte E-Mails oder Anmeldeseiten), um Zugangsdaten zu erlangen. Eine Phishing-resistente Multi-Faktor-Authentifizierung (MFA) minimiert die Wirksamkeit solcher Angriffe.

- **Push-Benachrichtigung** — Eine Authentifizierungsmethode, bei der der Nutzer einen Anmeldeversuch über eine Benachrichtigung in der mobilen App bestätigt. Diese kann zusätzlich durch Biometrie und einen Nummernabgleich gesichert werden.

- **Push bombing** — eine Angriffstechnik, bei der ein Angreifer den Benutzer mit einer Flut von Push-Benachrichtigungen bombadiert, um eine versehentliche Bestätigung zu erzwingen. Dem wird durch Mechanismen wie den Nummernabgleich entgegengewirkt.

- **RADIUS (Remote Authentication Dial-In User Service)** — Ein Kommunikationsprotokoll zur Authentifizierung, Autorisierung und Abrechnung des Benutzerzugriffs auf Computernetzwerke. Es wird häufig zur Integration von MFA-Systemen mit VPNs, WLAN-Systemen und Terminalservern verwendet.

- **Remote Desktop Protocol (RDP)** — Microsoft-Protokoll zur Ermöglichung der Remote-Verbindung mit dem Desktop eines anderen Computers. Aus Sicherheitsgründen sollten RDP-Verbindungen aufgrund ihrer häufigen Nutzung bei Fernangriffen mit MFA gesichert werden.

- **REST-API (Representational State Transfer Application Programming Interface)** — Eine REST-basierte Programmierschnittstelle, die es Systemen ermöglicht, über HTTP-Protokolle zu kommunizieren. Wird häufig zur Integration von MFA-Systemen mit proprietären Anwendungen, Portalen und Cloud-Diensten verwendet.

- **DSGVO (Datenschutz-Grundverordnung)** — Die EU-Verordnung 2016/679 zum Schutz personenbezogener Daten verpflichtet Verantwortliche und Auftragsverarbeiter zur Umsetzung „geeigneter technischer und organisatorischer Maßnahmen“ zum Schutz personenbezogener Daten. Obwohl die Multi-Faktor-Authentifizierung (MFA) nicht explizit erwähnt wird, gilt sie im Kontext des Schutzes des Zugangs zu personenbezogenen Daten weithin als verhältnismäßige Maßnahme.

- **SAML (Security Assertion Markup Language)** — Informationsaustauschstandard
  Es geht um Authentifizierung und Autorisierung zwischen einem Identitätsanbieter (IdP) und

einem Dienstanbieter (SP). Wird häufig zur Integration von Single Sign-On (SSO)- und MFA-Systemen verwendet in Unternehmensumgebungen.

- **SIEM (Security Information and Event Management)** — Ein System zur zentralen Erfassung, Korrelation und Analyse von Protokollen und Sicherheitsereignissen. Die Integration der MFA-Plattform in ein SIEM-Tool ermöglicht eine einfachere Überprüfung von Anmeldungen und die Erkennung von Unregelmäßigkeiten.

- **Single Sign-On (SSO)** — ein Single-Sign-On-Mechanismus, bei dem sich ein Benutzer nur einmal anmeldet und Zugriff auf mehrere Anwendungen erhält, ohne die Anmeldeinformationen erneut eingeben zu müssen.

- **Time-Based One-Time Password (TOTP)** — eine zeitbasierte Methode zur Generierung von Einmalcodes, die dem RFC-6238-Standard entspricht. Die Codes ändern sich alle 30 Sekunden und werden lokal in der Anwendung generiert (z. B. Google Authenticator, Rublon Authenticator).

- **Windows Logon (Anmeldung bei Windows)** — Der Prozess der Benutzerauthentifizierung beim Anmelden am lokalen Windows-Betriebssystem. Es unterstützt standardmäßig keine Multi-Faktor-Authentifizierung (MFA), kann aber durch zusätzliche Lösungen wie Rublon MFA abgesichert werden.

- **Zero Trust** — Ein Sicherheitsmodell, bei dem keiner Identität oder keinem Gerät automatisch vertraut wird, selbst wenn es sich im internen Netzwerk befindet. Multi-Faktor-Authentifizierung (MFA) ist eine Schlüsselkomponente einer Zero-Trust-Architektur und gewährleistet eine starke Benutzerauthentifizierung.

**Rublon sp. z o.o.**
ul. Stanislawa Wyspianskiego 11
65-036 Zielona Gora
Polen

**www.rublon.de**