CENTRE FOR CYBERSECURITY BELGIUM

MULTI-FAKTOR-AUTHENTIFIZIERUNG (MFA): EIN LEITFADEN FÜR ORGANISATIONEN

VERSTEHEN UND IMPLEMENTIEREN DER MFA FÜR MEHR IT-SICHERHEIT

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Inhaltsverzeichnis

1. Einleitung

Wenn es um die Sicherheit Ihrer Konten geht, haben Sie wahrscheinlich schon von der Zwei-Faktor-Authentifizierung (2FA) oder der Multi-Faktor-Authentifizierung (MFA) gehört. Die Zwei-Faktor-Authentifizierung ist ein Sicherheitskonzept, bei dem für den Zugriff auf ein Konto zwei Faktoren zur Authentifizierung erforderlich sind. Die Multi-Faktor-Authentifizierung (MFA) erfordert die Vorlage von zwei oder mehr Nachweisen bzw. Faktoren zwecks Authentifizierung. Während die 2FA also zwei Verifizierungsschritte umfasst, geht die MFA einen Schritt weiter, indem sie mehrere Authentifizierungsmethoden einbezieht.

Diese einfache, aber robuste Lösung bietet einen zusätzlichen Schutz, da Sie zwei oder mehr Identifizierungsschritte machen müssen. Selbst wenn jemand Ihr Passwort kennt, verhindert eine aktivierte MFA den unbefugten Zugriff auf Ihre Konten. Es wird dringend empfohlen, die MFA zu aktivieren, wo immer dies möglich ist, da es einfach ist und die Sicherheit erhöht. Die Bedeutung der 2FA bzw. MFA für Organisationen, ob öffentliche oder private, kann nicht hoch genug eingeschätzt werden. Cyber-Bedrohungen, einschließlich Ransomware-Angriffe, Datenmissbrauch und Systemeinbrüche, stellen erhebliche Risiken dar. Statistiken zeigen, dass ein erheblicher Prozentsatz der Ransomware-Angriffe durch die Implementierung der MFA hätte verhindert werden können. Viele dieser Angriffe könnten mithilfe robuster Authentifizierungsmaßnahmen unterbunden werden. Durch das Hinzufügen mehrerer Sicherheitsebenen erschwert die MFA Cyberkriminellen den Zugang zu sensiblen Daten und verringert so die Wahrscheinlichkeit von Datenmissbrauch und anderen Cyberbedrohungen.

In diesem Leitfaden erläutern wir Ihnen die Grundlagen der MFA und geben Ihnen praktische Tipps für die Umsetzung in Ihrem Unternehmen. Wir werden auch Beispiele aus der Praxis erörtern und Tipps geben, wie Sie häufige Fallstricke beim Einsatz von MFA-Lösungen vermeiden können. Am Ende dieses Leitfadens werden Sie ein besseres Verständnis der MFA haben und wissen, wie Sie sie effektiv einsetzen können, um die sensiblen Daten Ihres Unternehmens zu schützen. In unserem Cyberfundamentals Framework betonen wir auch deutlich die entscheidende Rolle starker Authentifizierungsmaßnahmen für den Schutz der digitalen Werte Ihres Unternehmens.

2. Was ist die Multi-Faktor-Authentifizierung und warum ist sie wichtig?

Einfach ausgedrückt, bedingt die MFA beim Zugriff auf ein Konto oder System neben Ihrem Passwort die Verwendung eines zusätzlichen Codes oder einer Bestätigung. Bei der MFA müssen Sie ein Passwort und ein Token oder biometrische Daten angeben, um auf bestimmte Daten zuzugreifen, was das Risiko eines unbefugten Zugriffs erheblich verringert. Durch das Erfordernis mehrerer Authentifizierungsformen verbessert die MFA die Sicherheit Ihres Unternehmens erheblich und **verringert das Risiko eines unbefugten Zugriffs auf sensible Informationen oder Systeme**.

Um einen sicheren Zugang zu Ihrem Konto zu erhalten, müssen Sie sich ausweisen. Dies kann durch den Einsatz von drei Methoden oder Faktoren erreicht werden:

- etwas, das nur Sie kennen (Ihr Passwort oder Ihre PIN-Nummer);
- etwas, zu dem nur Sie Zugang haben (Ihr Telefon oder Token); oder
- etwas, das ein Teil von Ihnen ist (Ihr Fingerabdruck, Ihr Gesicht, Ihre Iris, usw.).

Die Implementierung der MFA auf Unternehmensebene bedeutet, dass Mitarbeiter und alle anderen Benutzer, die Zugang zu Ihren Ressourcen benötigen, mehr als einen einzigen Authentifizierungsschritt durchlaufen müssen, um auf Ihre Unternehmenssysteme, Netzwerke, sensible Informationen und Anwendungen zuzugreifen. Die MFA kann für zahlreiche Anwendungen und Systeme implementiert werden, z. B. für E-Mails, VPNs, Cloud-basierte Dienste und interne Netzwerke.

Die MFA erlangt in der heutigen Wirtschaft angesichts immer ausgefeilterer und häufigerer Cyber-Bedrohungen zusehends an Bedeutung. So wäre beispielsweise ein Phishing-Angriff, der einen Benutzer zur Preisgabe seines Passworts verleitet, gegen ein **MFA-geschütztes System** weniger effizient, da der Angreifer auch den Token oder die biometrischen Daten bereitstellen müsste, um einen Systemzugang zu erhalten. Auch ein Brute-Force-Angriff, bei dem mehrere Kennwortkombinationen ausprobiert werden, wäre gegen ein MFA-geschütztes System wesentlich weniger effizient, da der Angreifer eine weitere Authentifizierung durchlaufen müsste.

Die Implementierung der MFA verbessert nicht nur **die Sicherheit**, sondern kann **Organisationen auch dabei helfen, die gesetzlichen und regulatorischen Anforderungen** (z. B. DSGVO, NIS2) für starke Authentifizierungsmethoden zu erfüllen. Die MFA kann auch dazu beitragen, die Kontinuität des Geschäftsbetriebs aufrechtzuerhalten, indem sie Cyberattacken verhindert bzw. deren Auswirkungen abmildert, so dass Unternehmen ihren Betrieb mit minimalen Unterbrechungen fortführen können.

3. Multi-Faktor-Authentifizierung: eine wichtige Sicherheitsmaßnahme für Unternehmen

Während die MFA traditionell mit Großunternehmen in Verbindung gebracht wurde, ist sie mittlerweile **für Organisationen aller Größenordnungen zugänglich und erschwinglich**. Darüber hinaus sind einige MFA-Lösungen im kostengünstigen **Abonnement** erhältlich, wobei Unternehmen nur für das bezahlen, was sie benötigen. Was die Komplexität angeht, werden MFA-Lösungen zunehmend **benutzerfreundlich** und **einfacher zu implementieren**, wobei viele Anbieter leicht zu konfigurierende Plug-and-Play-Lösungen anbieten.

Einige MFA-Lösungen lassen sich sogar in bestehende Zugangsverwaltungssysteme integrieren, so dass sie ohne größere Änderungen in die bestehende Infrastruktur (z. B. Active Directory oder LDAP) integriert werden können. Sowohl LDAP als auch Active Directory werden für die Authentifizierung und Autorisierung verwendet und ermöglichen es Unternehmen, den Benutzerzugriff auf Systeme, Anwendungen und Daten zu kontrollieren. Durch die Integration von MFA-Lösungen in LDAP oder Active Directory können Unternehmen ihre Sicherheit verbessern und sich vor Cyber-Bedrohungen schützen, ohne ihre bestehende Infrastruktur komplett überarbeiten zu müssen. Durch die Einstufung der MFA als **kritische Sicherheitsmaßnahme** können Unternehmen gewährleisten, dass sie proaktive Maßnahmen zum Schutz ihrer Firma und der vertraulichen Kundendaten ergriffen haben. Insgesamt können Organisationen die MFA implementieren, um ihre Sicherheit zu verbessern und das Risiko eines unbefugten Zugriffs auf sensible Daten oder Systeme zu verringern.

Mit der MFA als **kritische Sicherheitsmaßnahme** können Unternehmen sicherstellen, dass sie proaktiv zum Schutz ihres Unternehmens und ihrer sensiblen Kundendaten beitragen. Insgesamt gewährleistet die Implementierung einer MFA eine verbesserte Unternehmenssicherheit und mindert das Risiko eines unbefugten Zugriffs auf sensible Informationen oder Systeme.

Warum es nicht mehr ausreicht, nur ein Passwort zu verwenden:

- Passwörter können leicht erraten werden, besonders wenn sie einfach und leicht zu merken sind. Aus diesem Grund verwenden viele Angreifer Brute-Force- und Passwort-Spraying-Angriffe, bei denen sie versuchen, ein Passwort zu erraten, indem sie so viele Kombinationen ausprobieren, bis sie es gefunden haben.
- Dieselben Passwörter werden teils für mehrere Konten wiederverwendet, d. h., wenn ein Passwort kompromittiert wird, können Angreifer es verwenden, um ebenfalls Zugang zu anderen Konten zu verschaffen. Diese Wiederverwendung gleicher Passwörter ist ein häufiges Problem, das die reine Passwortauthentifizierung weniger sicher macht.

Passwörter können **durch Phishing-Angriffe oder Malware gestohlen werden**. Die Täter können gefälschte E-Mails oder Nachrichten verschicken, die den Anschein erwecken, von einer legitimen Quelle zu stammen, und die Benutzer dazu verleiten, ihre Logins preiszugeben. Ebenso lassen sich Passwörter mit der geeigneten Malware direkt vom Gerät eines Benutzers stehlen.

Aufgrund dieser Schwächen kann **ein reiner Passwortschutz auf verschiedene Weisen ausgespielt werden**. So können Angreifer beispielsweise gestohlene oder erratene Passwörter verwenden, um sich Zugang zu den sensiblen Daten oder Systemen eines Unternehmens zu verschaffen. Sie können auch Tools zum Hacken von Passwörtern verwenden, um schwache Passwörter zu erkennen und diese dann für den Zugriff auf andere Konten verwenden. Zusammenfassend lässt sich sagen, dass die Schwächen von Passwörtern sie anfällig machen, weshalb die Implementierung einer MFA für die Verbesserung der Sicherheit entscheidend ist.

4. Wie implementiert man die Multi-Faktor-Authentifizierung am Arbeitsplatz?

In der Praxis umfasst die Implementierung der MFA für Unternehmen vier Schritte, um sicherzustellen, dass die Einführung effizient und sicher ist: Identifizierung, Auswahl, Planung und Implementierung.

Der erste Schritt besteht darin, **festzustellen, welche Systeme und Anwendungen eine MFA benötigen**, und welche Arten der Authentifizierung am praktikabelsten sind. Der Zugang zu vertraulichen Daten sollte über eine MFA gesichert werden.

Der zweite Schritt besteht darin, **eine MFA-Lösung auszuwählen, die für die Bedürfnisse und das Budget Ihres Unternehmens geeignet ist**. Für Unternehmen ist es wichtig, bei der Auswahl einer MFA-Lösung Faktoren wie Benutzerfreundlichkeit, Skalierbarkeit und Kosten zu berücksichtigen. Außerdem sollten Sie eine Lösung wählen, die mit den bestehenden Systemen und Anwendungen Ihres Unternehmens kompatibel ist, und die Sicherheitsrisiken und Bedrohungen berücksichtigt, denen Ihr Unternehmen ausgesetzt ist.

Hier sind einige konkrete Beispiele, die Unternehmen bei der Entscheidung für eine MFA-Lösung berücksichtigen können:

- **SMS-basierte MFA**: Dabei handelt es sich um eine Option, die einen einmaligen Code per SMS an das Telefon des Benutzers sendet. Der Benutzer gibt dann diesen Code ein, um die Authentifizierung abzuschließen.
- **Softwarebasierte MFA**: Bei dieser Option wird in der Regel eine mobile App oder eine Desktop-Software verwendet, um einen einmaligen Code zu generieren. Einige Beispiele für softwarebasierte MFA sind Google Authenticator und Microsoft Authenticator.
- **Hardware-basierte MFA**: Bei dieser Option wird in der Regel ein physisches Token, z. B. eine Smartcard oder ein USB-Gerät, verwendet, das einen einmaligen Code erzeugt. Hardware-basierte MFA kann teurer und weniger flexibel sein als andere Optionen, kann sich aber für Organisationen empfehlen, die ein höheres Maß an Sicherheit benötigen.
- **Biometrische MFA**: Dabei werden biometrische Daten, wie Fingerabdrücke oder Gesichtserkennung, zur Authentifizierung der Nutzer verwendet. Die biometrische MFA kann bequemer und sicherer sein als andere Lösungen, erfordert jedoch möglicherweise spezielle Hard- oder Software und kann teurer sein.

Der dritte Schritt ist die **Planung der Einführung der MFA-Lösung**. Dies ist wichtig, um sicherzustellen, dass die Einführung effizient verläuft und den Geschäftsbetrieb nicht stört. Organisationen sollten bei der Planung der Einführung auch Aspekte wie Benutzerschulung, Kommunikation und Support berücksichtigen. Es ist wichtig, den Nutzern die Vorteile der MFA zu vermitteln und Schulungen zur sachgerechten Nutzung der MFA-Lösung anzubieten.

Der letzte Schritt ist die Implementierung der MFA-Lösung . Dazu muss die MFA-Lösung so konfiguriert werden, dass sie mit den zuvor bestimmten Systemen und Anwendungen funktioniert. Die Unternehmen sollten den Nutzern auch fortlaufend Unterstützung anbieten, um sicherzustellen, dass die MFA-Lösung ordnungsgemäß verwendet wird, und um eventuell auftretende Probleme zu beheben.

Die Verbesserung der Cybersicherheit mag oft wie eine entmutigende und komplexe Aufgabe erscheinen, insbesondere bei begrenzten Ressourcen und Budgets. Die Implementierung der MFA kann jedoch eine schnelle und effektive Lösung sein, um Ihre Unternehmenssicherheit erheblich zu verbessern. Diese zusätzliche Sicherheitsebene verringert das Risiko eines unbefugten Zugriffs erheblich, da es für Angreifer sehr viel schwieriger ist, die herkömmlichen passwortbasierten Sicherheitsmaßnahmen zu umgehen. Die MFA kann einfach implementiert werden, da es am Markt viele benutzerfreundliche Lösungen gibt. Mithilfe der MFA-Implementierung können Unternehmen ihre Sicherheit umgehend verbessern, ihre sensiblen Daten schützen und das Vertrauen ihrer Kunden stärken – und das alles im Rahmen Ihrer Budgets und Ressourcen.

4.1 MULTI-FAKTOR-AUTHENTIFIZIERUNG AUF ANWENDUNGSEBENE

Die MFA kann für etliche Anwendungen und Systeme implementiert werden, z. B. für E-Mails, VPNs, Cloud-basierte Dienste und interne Netzwerke. Die am häufigsten genutzten Dienste bieten eine Form der Multi-Faktor-Verifizierung und haben eine kurze Anleitungsseite. Einige davon finden Sie hier:

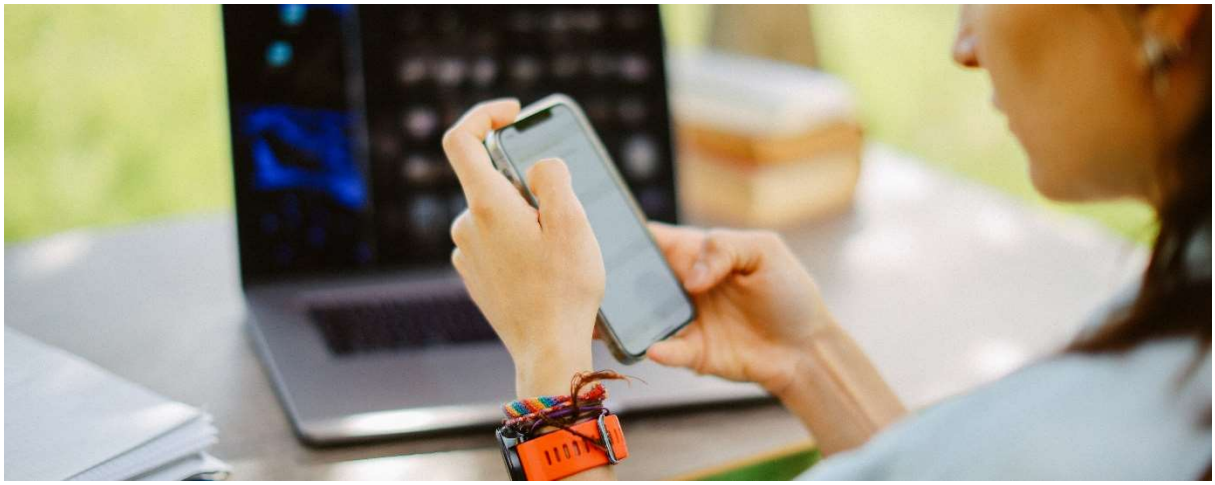
- Dropbox
- Google
- LinkedIn
- Microsoft
- Skype
- WhatsApp
- Yahoo

Für konkretere Beispiele verweisen wir Sie auf den folgenden Artikel: Ist die Zwei-Faktor-Authentifizierung umständlich in der Handhabung?

4.2 DIE MULTI-FAKTOR-AUTHENTIFIZIERUNG BEIM FERNZUGRIFF

Der Fernzugriff bezieht sich auf die Möglichkeit von Nutzern oder Prozessen, die in ihrem Namen handeln, eine Verbindung zu einem unternehmenseigenen IT-System über externe Netzwerke wie das Internet herzustellen. Er erfolgt in aller Regel über verschlüsselte virtuelle private Netzwerke (VPNs), um die Vertraulichkeit und Integrität der Kommunikation zu gewährleisten. Zur Implementierung eines sicheren Fernzugriffs müssen strenge Nutzungsbeschränkungen, Konfigurationsanforderungen und Autorisierungsprotokolle festgelegt werden, bevor solche Verbindungen zugelassen werden. Dadurch wird sichergestellt, dass sich nur autorisierte Benutzer per Fernzugriff in das System einloggen können, so dass letzteres vor potenziellen externen Bedrohungen geschützt wird.

Im Zusammenhang mit dem Fernzugriff kann die Bedeutung der MFA nicht hoch genug eingeschätzt werden. Ein Passwort allein, egal wie komplex es ist, kann immer von ambitionierten Cyberkriminellen gehackt, erraten oder



abgefischt werden. Durch die Implementierung der MFA können Unternehmen **eine zusätzliche Sicherheitsebene zu ihren Fernzugriffsprotokollen** hinzufügen und sicherstellen, dass nur autorisierte Benutzer auf ihre Systeme zugreifen können.

- **Sicherheit**: Wählen Sie ein sicheres MFA-Tool, das den Sicherheitsstandards und bewährten Verfahren entspricht.
- **Kompatibilität**: Achten Sie darauf, ein MFA-Tool zu wählen, das mit dem bestehenden System und der Infrastruktur Ihrer Organisation kompatibel ist (z. B. Betriebssystemversion) und das sich problemlos in den Authentifizierungsrahmen Ihrer Organisation integrieren lässt (z. B. Active Directory).
- **Implementierung**: Wählen Sie ein MFA-Tool, das Ihnen Sicherheit bietet, sich leicht in Ihre Unternehmensumgebung integrieren lässt und Ihnen das erforderliche Maß an Support bietet.
- **Kosten** : Bedenken Sie die Kosten der für die Implementierung der MFH erforderlichen Ressourcen wie Wartung, Lizenzgebühren usw.
- **Authentifizierungsoptionen**: Idealerweise wählen Sie ein MFA-Tool, das mehrere Authentifizierungsoptionen bietet, um den Benutzern die Flexibilität zu geben, die Authentifizierungsfaktoren entsprechend ihren Vorlieben und Bedürfnissen zu nutzen.

4.3 WICHTIGE ÜBERLEGUNGEN BEI DER AUSWAHL EINER MFA-LÖSUNG

Bevor Sie sich für eine MFA-Lösung entscheiden, sollten Sie folgende wichtige Aspekte berücksichtigen:

Nachfolgend finden Sie einige Beispiele für die Einrichtung der Multi-Faktor-Authentifizierung in Ihrem Unternehmen unter Verwendung der gängigsten Authentifizierungsanwendungen. Dabei handelt es sich um allgemeine Richtlinien, die möglicherweise nicht auf die spezifischen Bedürfnisse Ihres Unternehmens zutreffen oder sich je nach Umgebung ändern können.

4.4 IMPLEMENTIERUNG DER MFA IN AZURE CLOUD

Schritt 1: Azure Active Directory (Vorbedingung)

Um die Microsoft Authenticator-App verwenden zu können, muss Ihre Organisation über ein Azure AD (Active Directory)-Konto verfügen.

Schritt 2: Die MFA aktivieren

Jede Ausgabe von Azure AD enthält die Azure AD Multi-Faktor-Authentifizierung. Für eine Registrierungskampagne ist keine zusätzliche Lizenz erforderlich. Dies kann im Azure-Portal unter Azure Active Directory > Security > MFA erfolgen.

Schritt 3: Authentifizierungsmethoden wählen

Microsoft Authenticator unterstützt eine Reihe von Authentifizierungsmethoden, z. B. Push-Benachrichtigungen und Einmal-Passcodes.

Schritt 4: Richtlinien konfigurieren

In diesem Schritt kann Ihr Unternehmen festlegen, welche Benutzer die MFA verwenden müssen, welche Authentifizierungsmethoden verwendet werden können und wann die MFA erforderlich ist (z. B. bei einer bestimmten Anwendung).

Dies kann mit Hilfe einer der folgenden Richtlinien ermittelt werden:

- *MFA-Registrierungsrichtlinie*: Die Nutzer müssen für die Benachrichtigung über die mobile Anwendung freigeschaltet werden.
- *Richtlinien zu den Authentifizierungsmethoden*: Die Benutzer müssen für die Authenticator-App aktiviert und der Authentifizierungsmodus auf Beliebig oder Push eingestellt sein.

Schritt 5: Microsoft-Authentifikator einrichten

Sobald die MFA aktiviert und die Richtlinien konfiguriert sind, können die Anweisungen zur Einrichtung der Microsoft-Authentifizierung den Benutzern per E-Mail oder über die internen Kommunikationsplattformen Ihres Unternehmens (z. B. Intranet) mitgeteilt werden.

Weitere Hinweise finden Sie unter:

- Benutzer zur Einrichtung von Microsoft Authenticator anregen - Microsoft Entra | Microsoft Learn
- Konfigurieren Sie die MFA-Registrierungsrichtlinie – Azure Active Directory Identity Protection - Microsoft Entra | Microsoft Learn

4.5 IMPLEMENTIERUNG DER MFA IN GOOGLE CLOUD

Schritt 1: Google Cloud-Konto (Voraussetzung)

Um Google Authenticator verwenden zu können, muss Ihr Unternehmen über ein Google Cloud-Konto für die MFA-Bereitstellung verfügen.

Schritt 2: Zwei-Schritte-Verifizierung einrichten

Aktivieren Sie die 2-stufige Überprüfung über die Google Admin Console:

Menu > Security> Authentication > 2-step verification.

Schritt 3: Auswahl der Authentifizierungsmethode

Google Authenticator unterstützt eine Reihe von Authentifizierungsmethoden für die 2-Schritt-Verifizierung wie Google Authenticator App (für Android Version 4.4 und höher), Sicherheitsschlüssel, Google Prompt, Textnachricht oder Telefonanruf und Backup-Codes.

Schritt 4: Richtlinien konfigurieren

Bestimmen Sie, welche Benutzer die MFA verwenden müssen. Um die Einstellung auf alle anzuwenden, lassen Sie die oberste Organisationseinheit ausgewählt. Andernfalls wählen Sie eine untergeordnete Organisationseinheit oder eine Konfigurationsgruppe aus und aktivieren Sie das Kontrollkästchen Benutzern die Aktivierung der 2-Schritte-Verifizierung erlauben.

Um die MFA für alle Benutzer oder die ausgewählte Gruppe durchzusetzen, aktivieren Sie die Durchsetzungsoption.

Schritt 5: Anmeldung 2-Schritte-Verifizierung

Übermitteln Sie den Nutzern eine Anleitung zur Einrichtung von Google Authenticator per E-Mail oder über die internen Kommunikationsplattformen Ihrer Organisation.

Weitere Hinweise finden Sie unter: 2-Schritt-Verifizierung bereitstellen - Google Workspace Admin-Hilfe

4.6 IMPLEMENTIERUNG DER MFA IN BENUTZERDEFINIERTEN APPS MIT ITSME

Schritt 1: Registrierung für die itsme MFA-Dienste

Ihre Organisation muss für die itsme MFA-Dienste registriert sein, um die MFA mit der itsme-Anwendung zu aktivieren und ein Konto auf dem itsme-Verwaltungsportal zu erstellen, mit dem Ihre Organisation die MFA-Einstellungen verwalten und Nutzungsstatistiken einsehen kann.

Schritt 2: Wählen Sie die Authentifizierungsmethode

Die in itsme verfügbaren Authentifizierungsmethoden basieren zumindest auf der Kombination von etwas, das der Nutzer besitzt, wie z. B. sein Smartphone und die installierte itsme-Anwendung, und den biometrischen Daten des Nutzers, wie z. B. Fingerabdruck oder Face ID, oder etwas, das der Nutzer kennt (z. B. PIN-Code).

Schritt 3: Richtlinien konfigurieren

Navigieren Sie zu den Richtlinieneinstellungen im Administrationsportal und legen Sie die Regeln fest, die bestimmen, wann die itsme-MFA erforderlich ist, sowie Ausnahmen und die Einrichtung einer Benachrichtigung im Falle fehlgeschlagener Anmeldeversuche.

Schritt 4: Anmeldung für die MFA

Übermitteln Sie den Nutzern eine Anleitung zur Einrichtung von itsme per E-Mail oder über die internen Kommunikationsplattformen Ihrer Organisation.

Weitere Hinweise finden Sie unter: Allgemeine Informationen - Dokumentation - Onboarding (belgianmobileid.be)

4.7 AUTHENTICATOR-ANWENDUNGEN

Eine Authenticator-App ist eine Anwendung, mit der zeitbasierte Einmalpasswörter (TOTPS) für die Multi-Faktor-Authentifizierung generiert werden. Sie hilft den Nutzern, ihre Konten zu sichern, indem sie eine zweite Verifizierungsebene bietet.

- Authy
- Google-Authentifikator
- Microsoft-Authentifikator
- Okta Verify

5. Überlegungen zur Konfiguration der Multi-Faktor-Authentifizierung und Benutzersupport

Richtlinienkonfiguration:

- Bestimmen Sie die zulässige Authentifizierungsmethode, die von der gewählten Authentifizierungsanwendung bereitgestellt wird und mit der Umgebung Ihrer Organisation und den Benutzeranforderungen kompatibel ist.
- Es wird empfohlen, die MFA-Authentifizierung für alle Benutzer und Anwendungen vorzusehen, insbesondere bei Telearbeit. Bei diesem Verfahren muss der Administrator festlegen, für welche Benutzer, Gruppen und Anwendungen die MFA gelten soll, Kriterien für Ausnahmen definieren und sicherstellen, dass die entsprechenden Kontrollen vorhanden sind.
- Integrieren Sie die MFA in das in Ihrem Unternehmen vorhandene System, wie z. B. Active Directory, um sicherzustellen, dass die MFA für alle Anwendungen und Systeme eingesetzt wird, und sorgen Sie mithilfe eines einzigen Satzes von Anmeldedaten für ein hohes Sicherheitslevel und gleichzeitig für ein gutes Benutzererlebnis.

Benutzersupport:

Nach Konfiguration der Richtlinien und Einführung der MFA können sich Benutzer ohne die MFA nicht mehr im System anmelden. Ihre Organisation muss dafür sorgen, dass die Nutzer die entsprechende Unterstützung erhalten:

- Kommunizieren Sie klar und deutlich den Anmeldevorgang für die MFA und übermitteln Sie den Nutzern die Richtlinien für die Einrichtung der Authentifizierungs-App auf ihren mobilen Geräten mit Hilfe der Kommunikationskanäle Ihres Unternehmens wie E-Mail und Intranet.
- Führen Sie Benutzerschulungen durch, um das Bewusstsein für die MFA, ihren Zweck und ihre Verwendung zu schärfen.
- Bieten Sie kontinuierlichen Support mit Kontaktpersonen an, so dass die Nutzer diese bei der Implementierung um Hilfe bitten können.
- Halten Sie die Nutzer über Änderungen oder Aktualisierungen der MFA-Richtlinien und deren Anwendbarkeit auf dem Laufenden.

6. Potenzielle Probleme oder Hindernisse

6.1 KEINE VERBINDUNG

Es ist wichtig, einen Notfallplan zu haben, was zu tun ist, wenn ein Benutzer sich nicht mit der MFA authentifizieren kann, weil die Verbindung unterbrochen ist, das MFA-fähige Gerät verloren wurde oder er sich nicht mit der primären Methode authentifizieren kann (z. B. blockierte Handynummer, geänderte E-Mail). Dies kann Folgendes umfassen:

- Bereitstellung einer **Backup-Authentifizierungsmethode** wie einer zweiten Telefonnummer oder E-Mail-Adresse.
- Verwendung **alternativer Authentifizierungsmethoden** , die nicht auf eine Online-Verbindung angewiesen sind (z. B. physische Token, Smartcards).
- **Vorübergehende Deaktivierung** der MFA für einen bestimmten Benutzer oder eine Gruppe von Benutzern. Dies sollte nur als letztes Mittel eingesetzt werden. Die MFA muss wieder aktiviert werden, sobald das Problem behoben ist.

Darüber hinaus sollte ein Leitfaden zur Betriebsunterstützung erstellt werden, der Schritt-für-Schritt-Anweisungen enthält, wie das Problem zu beheben ist, an wen man sich wenden kann und wie sichergestellt wird, dass die Daten Ihres Unternehmens während des Ausfalls gesichert bleiben.

6.2 FAKTOREN, DIE BEI DER WAHL EINER MFA-LÖSUNG ZU BERÜCKSICHTIGEN SIND

Bei der Auswahl einer Multi-Faktor-Authentifizierungslösung ist es wichtig, die Art der MFA zu berücksichtigen, die am besten zu den Anforderungen Ihres Unternehmens passt. Eine der am häufigsten verwendeten MFA-Methoden ist die Verwendung einer Authentifizierungs-App. Diese Methode ist zwar bequem und sicher, aber es ist wichtig zu bedenken, dass alle Nutzer ein Smartphone benötigen, um sie zu verwenden. Dies kann ein potenzielles Problem für **Organisationen sein, die ihren Mitarbeitern kein eigenes Smartphone zur Verfügung stellen** oder für **Mitarbeiter, die kein Smartphone besitzen**, oder **die Anwendung nicht auf ihrem persönlichen Smartphone installieren wollen oder nur begrenzten Zugang zu einem solchen haben** . In diesen Fällen kann es notwendig sein, alternative MFA-Methoden in Betracht zu ziehen, z. B. ein physisches Sicherheits-Token oder ein auf Textnachrichten basierendes System, um sicherzustellen, dass alle Benutzer sicher auf die Systeme zugreifen können. Daher ist es von entscheidender Bedeutung, **die Vor- und Nachteile** verschiedener MFA-Methoden abzuwägen, bevor eine Entscheidung getroffen wird, und sicherzustellen, dass die gewählte Lösung von allen Nutzern verwendet werden kann.

6.3 MFA UND BYOD

Persönliche Geräte wie Smartphones, die zu Arbeitszwecken verwendet werden, sind möglicherweise nicht mit der von Ihrem Unternehmen gewählten MFA-Methode kompatibel, was es schwierig macht, die **MFA in einer Bring Your Own Device (BYOD)-Umgebung** durchzusetzen und eine formal konsistente und korrekte MFA-Implementierung auf allen Geräten sicherzustellen.

Daher sollte Ihr Unternehmen den Einsatz eines Mobile Device Managements (MDM) in Erwägung ziehen, um die persönlichen Geräte der Benutzer, die zu Arbeitszwecken verwendet werden, zu verwalten und sicherzustellen, dass diese Geräte ordnungsgemäß gesichert sind und den Sicherheitsrichtlinien Ihres Unternehmens entsprechen.

Darüber hinaus sollten die Sicherheitsrichtlinien Ihrer Organisation folgende Aspekte abdecken:

- Gewähr, dass die **Mindestsicherheitsanforderungen** in den Geräten der Nutzer umgesetzt wurden (z. B. Art des Betriebssystems, Anforderungen an die Aktualisierung des Geräts mit Sicherheits-Patches, Konfigurationen usw.).
- Unterstreichung der Bedeutung der MFA und **der mit der Verwendung privater Geräte** für Arbeitszwecke verbundenen Risiken. Diese Richtlinien sollten allen Mitarbeitern mitgeteilt werden, um das Bewusstsein dafür zu schärfen, wie persönliche Geräte, die zu Arbeitszwecken verwendet werden, zu schützen sind.
- Den Nutzern sollte Unterstützung in Form von **klaren Richtlinien** geboten werden, damit sie ihre Geräte sachgemäß für die Verwendung der MFA konfigurieren können, sowie Verfahren, wie und wo sie im Falle eines Sicherheitsvorfalls im Zusammenhang mit BYOD Meldung machen können.
- Begrenzen Sie den Fernzugriff. Ihr Unternehmen sollte zudem in Erwägung ziehen, den **Zugang zu Daten und Anwendungen je nach Risikoniveau zu segmentieren** und die MFA vorzuschreiben, wann immer dies machbar ist, insbesondere bei Daten und Anwendungen mit hohem Risiko und bei Fernzugriffen.

Zusammenfassend lässt sich sagen, dass die Implementierung der **MFA in BYOD-Umgebungen** als wesentliche Sicherheitsmaßnahme betrachtet werden sollte, da die Geräte der Mitarbeiter möglicherweise nicht dieselben Sicherheitsstandards erfüllen wie die unternehmenseigenen Geräte.

7. Wichtige Überlegungen für eine sichere MFA-Nutzung

Beim Einsatz einer MFA, um eine zusätzliche Schutzebene hinzuzufügen und die Sicherheit zu erhöhen, ist es wichtig, wachsam zu bleiben und bestimmte Überlegungen zu beachten:

- **Gewährleistung der Gerätesicherheit**: Implementieren Sie Sicherheitsupdates und Patches für Ihre MFA-Anwendung, Betriebssysteme und Softwareversionen, die auf Ihren Geräten installiert sind, sobald sie verfügbar sind, um potenzielle Schwachstellen zu beheben.
- **Achtsame Interaktion**: Wenn Sie sich für Push-up-Benachrichtigungen als zweiten Authentifizierungsfaktor entscheiden, ist es wichtig, wachsam zu bleiben und zu vermeiden, dass Sie Benachrichtigungen gedankenlos akzeptieren, ohne den Inhalt zu prüfen. Nehmen Sie sich immer die Zeit, die Meldung zu lesen, bevor Sie etwas unternehmen.
- **Verwenden Sie ein starkes Passwort bzw. eine starke Umschreibung:** Verwenden Sie zusätzlich zur MFA ein starkes und langes Passwort oder eine Sammlung von mindestens drei zufälligen, gebräuchlichen Wörtern, die zu einem Satz kombiniert werden und eine sehr gute Kombination aus Einprägsamkeit und Sicherheit bieten, mit Klein- und Großbuchstaben, möglicherweise auch Zahlen und Sonderzeichen, und vermeiden Sie offensichtliche Codes wie „Passwort“, Buchstaben- oder Zahlenfolgen und persönliche Informationen.
- **Offizielle Plattformen verwenden:** Verwenden Sie beim Herunterladen von MFA-Anwendungen vertrauenswürdige offizielle App-Stores wie Google Play Stores für Android- oder den Apple App Store für iOS-Geräte, um die Authentizität und Integrität der Anwendung sicherzustellen und das Risiko des Herunterladens von Schadsoftware zu minimieren.

8. Referenzen

8.1 CYBERFUNDAMENTALS

Dieser Anhang verweist auf die relevanten grundlegenden Cyberfundamental-Anforderungen im Zusammenhang mit der Multi-Faktor-Authentifizierung (MFA) und bietet eine detaillierte Referenz zur Unterstützung der Implementierung und Administration der MFA in unserem Cybersicherheitsrahmen.

- **PR.AC-3**: **Der Fernzugriff wird verwaltet.**

  Key Measure: Der Fernzugriff auf die Netze der Organisation muss gesichert sein, **unter anderem durch eine Multi-Faktor-Authentifizierung (MFA)**.

8.2 SAFEONWEB (@WORK)

Konten mit Multi-Faktor-Authentifizierung schützen | Safeonweb@work

Ein starkes Passwort zum Schutz wertvoller Informationen | Safeonweb@work

Zugangsregelung | Safeonweb@work

Zwei-Faktor-Authentifizierung nutzen | Safeonweb

Ist die Zwei-Faktor-Authentifizierung umständlich? | Safeonweb