MULTI-FAKTOR-AUTHENTIFIZIERUNG
IM MICROSOFT 365 UMFELD

EIN MUSS FÜR EINEN EFFEKTIVEN SCHUTZ

Wie Multi-Faktor-Authentifizierung die Sicherheit im Microsoft 365 Umfeld erhöht

Angesichts des stetigen Anstiegs der Bedrohung durch Cyberkriminalität ist es für Unternehmen von entscheidender Bedeutung, ihre Sicherheitsvorkehrungen kontinuierlich zu verbessern. Dabei ist es unerlässlich, proaktiv zu handeln und robuste Sicherheitsmaßnahmen zu implementieren – auch im Microsoft 365 Umfeld.

In vielen Unternehmen ist die einstufige Authentifizierung Standardpraxis. Mitarbeiter melden sich lediglich mit einem Benutzer-namen und Passwort an, um auf ihre Konten zuzugreifen. Doch diese Methode erweist sich zunehmend als unsicher und öffnet Tür und Tor für Cyberkriminalität. Angreifer entwickeln konstant neue Methoden, um Passwörter zu knacken und sich unbefugten Zugang zu Accounts zu verschaffen.

Obwohl Microsoft bereits Sicherheitsstandards eigenständig umsetzt und Unternehmen diese nur noch aktivieren müssen, sind weitere Maßnahmen erforderlich, um Bedrohungen effektiv zu bekämpfen.

Eine vielversprechende Lösung zur Verbesserung der Kontosicherheit ist die Multi-Faktor-Authentifizierung (MFA). Diese Methode fordert Benutzer während des Anmeldevorgangs auf, zusätzliche Identifizierungsverfahren durchzuführen, was die Sicherheit erheblich erhöht.

Microsoft hat wiederholt betont, wie wichtig die Umstellung auf eine Zwei-Faktor-Authentifizierung ist. Laut ihren Statistiken von Anfang 2020 verfügten über 99,9 %* der kompromittierten Konten nicht über MFA, was sie anfällig für Angriffe wie Kennwort-Spraying, Phishing und die Wiederverwendung von Passwörtern macht.

(*Ursprungs-Quelle: https://learn.microsoft.com/de-de/partner-center/security-at-your-organization vom 19.01.2024)

Doch was genau ist MFA und wie funktioniert es?

Bei der Multi-Faktor-Authentifizierung müssen Benutzer mehr als nur den Benutzernamen und das Passwort angeben, um sich anzumelden. Zusätzlich zu diesen Informationen müssen sie eine weitere Form der Identifizierung verwenden, die auf unterschiedlichen Faktoren basiert. Dies kann beispielsweise ein per App generierter Token oder ein per SMS gesendeter Code sein. Die Kombination dieser verschiedenen Identifizierungsmethoden erschwert es Cyberkriminellen erheblich, Zugriff auf Nutzerkonten zu erlangen.

Wie gehen Cyberkriminelle vor?

Cyberkriminelle nutzen verschiedene Techniken, um sich unbefugten Zugang zu Benutzerkonten zu verschaffen.

Einige der häufigsten Methoden sind:

- Passwort-Spraying: Bei dieser Technik werden gängige Passwörter mit riesigen Listen verschiedenster Nutzernamen durchprobiert. Wenn das Programm oder der Angreifer einen Treffer erzielt, erhalten sie Zugriff auf das Benutzerkonto. Von dort aus können sie Daten auslesen oder sogar Malware nachladen und installieren.

- Passwort-Replay: Diese Methode nutzt die Tatsache aus, dass viele Nutzer ihre Passwörter mehrfach verwenden, um sie sich besser merken zu können. Wenn Zugangsdaten von Nutzern auf einem beliebten Anmeldeportal gehackt und im großen Stil gehandelt wurden, werden dieselben Zugangsdaten oft auf anderen Plattformen ausprobiert. Dies kann zu erstaunlich vielen Erfolgen führen und verdeutlicht die Gefahr der Passwort-Wiederverwendung.

Risiken & Folgen

Die Risiken und Folgen einer unzureichenden Sicherheit von M365 Konten sind vielfältig und können schwerwiegende Auswirkungen auf Unternehmen und ihre Kunden haben:

- Zugriff auf Adressbücher: Cyberkriminelle könnten Zugriff auf Adressbücher erlangen und sensible Kontaktdaten von Mitarbeitern und Kunden stehlen. Diese Daten könnten für gezielte Phishing-Angriffe verwendet werden, um weitere Benutzerkonten und damit weitere persönliche Informationen abzufangen.

- Datenzugriff auf SharePoint: Durch den unbefugten Zugriff auf SharePoint-Dateien könnten Cyberkriminelle vertrauliche Unternehmensdaten einsehen, herunterladen oder manipulieren. Dies kann zu erheblichen Datenschutzverletzungen führen und das Vertrauen von Kunden und Geschäftspartnern beeinträchtigen.

- Versenden von Teams-Nachrichten: Cyberkriminelle könnten sich Zugriff auf Messaging-Plattformen wie Microsoft Teams verschaffen und gefälschte Nachrichten im Namen von Mitarbeitern oder Führungskräften versenden. Dies kann zu Verwirrung innerhalb des Unternehmens führen und sogar zu rechtlichen Konsequenzen führen.

- Wert von Datensätzen im Darknet: Die gestohlenen Daten könnten auf dem Darknet verkauft werden, wo sie einen erheblichen Wert haben. Persönliche Informationen, Unternehmens-dokumente und Zugangsdaten können von Cyber-kriminellen für verschiedene illegale Zwecke genutzt werden, einschließlich Identitätsdiebstahl, Betrug und Erpressung.

Sicherheitsmaßnahmen einfach umgesetzt

Die Implementierung von MFA bietet Unternehmen eine effektive Möglichkeit, ihre Sicherheitsstandards zu erhöhen und sich vor den wachsenden Bedrohungen des Cyberraums zu schützen. Dabei kann die Multi-Faktor-Authentifizierung verschieden aktiviert werden:

- Aktivierung über die mehrstufige Authentifizierung in Entra ID:
  Eine Möglichkeit zur Implementierung von MFA ist die Nutzung der mehrstufigen Authentifizierung im Entra ID über Conditional Access. Hierbei können Unternehmen beispielsweise vertrauenswürdige IP-Adressen definieren, bei denen kein zweiter Authentifizierungsfaktor erforderlich ist. Dies bietet eine bequeme Lösung für Mitarbeiter, die von bekannten Standorten aus auf Microsoft 365 zugreifen. Zusätzlich können Benutzer ihre Endgeräte als sicher markieren, wodurch der zweite Faktor für Anmeldungen von diesen Geräten für einen festgelegten Zeitraum nicht abgefragt wird.

- Aktivierung der Security Defaults im Tenant:
  Eine weitere Option ist die Aktivierung der Security Defaults von Microsoft auf Tenant-Ebene. Diese Einstellung erfordert die Registrierung für MFA für alle Benutzer und Administratoren und blockiert legacy Authentifizierungen, die keine moderne Authentifizierung verwenden. Während bei dieser Methode keine vertrauenswürdigen IP-Adressen konfiguriert werden können, steht den Benutzern als zweiter Authentifizierungsfaktor ausschließlich die Authenticator App zur Verfügung.

Datenschutzrechtliche Aspekte

Die Verwendung von Multifaktor-Authentifizierung im Microsoft 365 Umfeld bringt datenschutzrechtliche Aspekte mit sich, die beachtet werden müssen. Wichtige Punkte sind:

- Datenschutzrichtlinien: Die MFA muss den geltenden Datenschutzrichtlinien entsprechen, wie der DSGVO in der EU oder entsprechenden Gesetzen in Ihrer Region.

- Datenverarbeitungszwecke: Klären Sie die Zwecke der Datenverarbeitung im Zusammenhang mit MFA und minimieren Sie die Datenerfassung auf das Nötigste.

- Transparenz: Benutzer sollten über die Datensammlung, -verwendung und -speicherung im Rahmen von MFA informiert werden.

- Datensicherheit: Implementieren Sie angemessene Sicherheitsmaßnahmen wie Verschlüsselung und Zugriffsbeschränkungen, um gesammelte Daten zu schützen.

- Datenspeicherung: Begrenzen Sie die Datenspeicherung auf das Minimum und löschen Sie Daten, wenn sie nicht mehr benötigt werden.

- Rechte der Betroffenen: Benutzer sollten ihre Rechte bezüglich ihrer personenbezogenen Daten ausüben können.
  Datenübertragung: Achten Sie darauf, dass bei der Übertragung personenbezogener Daten in Drittländer angemessene Datenschutzmaßnahmen getroffen werden.

FIS-ASP Application Service Providing
und IT-Outsourcing GmbH
Röthleiner Weg 4
D-97506 Grafenrheinfeld
www.fis-asp.de