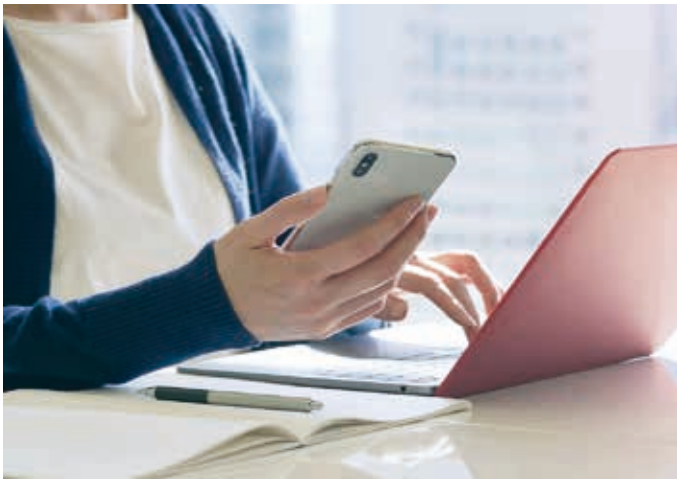
Kommunalreport | Ausgabe 2.2024

Ihre Sicherheit und unsere Datensicherheit

Zwei-Faktor-Authentifizierung

In der heutigen digitalen Welt ist der Schutz sensibler Daten von größter Bedeutung. Eine der effektivsten Methoden, um die Sicherheit sowohl persönlicher als auch dienstlicher Daten zu gewährleisten, ist die Zwei-Faktor-Authentifizierung (2FA). Besonders relevant wird dieses Thema, wenn dienstliche Daten auf privaten mobilen Geräten genutzt werden. Doch was genau ist 2FA und warum ist sie so wichtig?



Was ist Zwei-Faktor-Authentifizierung?

Die Zwei-Faktor-Authentifizierung ist ein Sicherheitsverfahren, das zwei verschiedene und unabhängige Faktoren zur Verifizierung der Identität eines Benutzers erfordert.

Diese Faktoren können in drei Kategorien unterteilt werden:

1. » **Wissen:** Etwas, das nur der Benutzer weiß (z. B. ein Passwort).
2. » **Besitz:** Etwas, das nur der Benutzer hat (z. B. ein Smartphone oder ein Token).
3. » **Inhärenz:** Etwas, das der Benutzer ist (z. B. ein Fingerabdruck oder eine Gesichtserkennung).

Durch die Kombination von zwei dieser Faktoren wird die Sicherheit erheblich erhöht, da ein Angreifer beide Faktoren überwinden müsste, um Zugang zu den geschützten Daten zu erhalten. Erst nach der Prüfung der zwei Faktoren wird der Zugriff freigegeben. Aktuell gilt die 2FA als das Mittel der Wahl, um die Sicherheit beim Authentifizierungsprozess zu maximieren.

Stand der Technik bei der Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (2FA) hat sich in den letzten Jahren stetig weiterentwickelt und bietet heute eine Vielzahl an Methoden, die den Schutz sensibler Daten noch effektiver gestalten. Besonders hervorzuheben sind dabei die folgenden aktuellen Entwicklungen:

» **1. Biometrische Verfahren:**
Die Nutzung biometrischer Merkmale wie Fingerabdruck, Gesichtserkennung oder Iris-Scan hat sich als besonders sicher erwiesen. Diese Verfahren sind schwer zu fälschen und bieten daher einen hohen Schutz gegen unbefugten Zugriff.

» **2. Hardware-gestützte Authentifizierung:**
Sicherheits-Token und USB-Schlüssel, wie zum Beispiel YubiKeys, bieten eine robuste Lösung für die 2FA. Diese Geräte generieren Einmalpasswörter oder nutzen kryptografische Schlüssel, um die Identität des Benutzers zu verifizieren.

» **3. Push-Benachrichtigungen:**
Moderne 2FA-Systeme nutzen Push-Benachrichtigungen, die an das Smartphone des Benutzers gesendet werden. Diese Methode ist benutzerfreundlich und bietet eine zusätzliche Sicherheitsebene, da sie eine direkte Interaktion des Benutzers erfordert.

» **4. Adaptive Authentifizierung:**
Diese fortschrittliche Methode passt das Authentifizierungsverfahren an das Verhalten des Benutzers an. Beispielsweise kann das System bei ungewöhnlichen Anmeldeversuchen zusätzliche Sicherheitsfragen stellen oder eine biometrische Verifizierung verlangen.

» **5. Integration in Mobile Device Management (MDM):**
Die Integration von 2FA in MDM-Lösungen ermöglicht eine zentrale Verwaltung und Durchsetzung von Sicherheitsrichtlinien auf mobilen Geräten. Dies ist besonders wichtig für Unternehmen, die private Geräte für dienstliche Zwecke zulassen.

Durch die kontinuierliche Weiterentwicklung und Anpassung der 2FA-Technologien können wir sicherstellen, dass unsere Daten auch in Zukunft bestmöglich geschützt sind. Es ist daher ratsam, stets auf dem neuesten Stand der Technik zu bleiben und die verfügbaren Sicherheitsmaßnahmen konsequent zu nutzen.

„Wir sind uns der Verantwortung bewusst, die mit dem Schutz sensibler Daten einhergeht, und setzen alles daran, diese Verantwortung ernst zu nehmen.“

Passkeys und ihre Rolle in der Authentifizierung

Eine interessante Neuerung im Bereich der Authentifizierung sind Passkeys. Diese ermöglichen es Nutzerinnen und Nutzern, sich bei Konten und Anwendungen anzumelden, ohne ein Passwort eingeben zu müssen. Stattdessen verwenden Passkeys Methoden wie die Eingabe eines Passcodes, biometrische Daten (z. B. Gesichtserkennung oder Fingerabdruck) oder ein Wischmuster, um Geräte zu entsperren.

Der wesentliche Unterschied zwischen Passkeys und der Zwei-Faktor-Authentifizierung besteht darin, dass Passkeys die Notwendigkeit eines Passworts vollständig eliminieren. Während 2FA eine zusätzliche Sicherheitsebene durch eine zweite Authentifizierungsmethode neben dem Benutzernamen und Passwort bietet, machen Passkeys Passwörter überflüssig. Dadurch stellen Passkeys eine benutzerfreundliche und sichere Alternative zu traditionellen Passwörtern dar und können in vielen Fällen die Notwendigkeit einer zusätzlichen 2FA-Methode ersetzen.

Mobile Geräte und dienstliche Daten

Die Nutzung privater mobiler Geräte für dienstliche Zwecke bringt zusätzliche Sicherheitsrisiken mit sich. Hier sind einige Best Practices, um die Sicherheit zu gewährleisten:

- **Geräteverschlüsselung:**
  Stellen Sie sicher, dass alle Daten auf dem Gerät verschlüsselt sind.
- **Regelmäßige Updates:**
  Halten Sie das Betriebssystem und alle Apps auf dem neuesten Stand.
- **Sichere Netzwerke:**
  Vermeiden Sie die Nutzung öffentlicher WLAN-Netzwerke für dienstliche Zwecke.
- **Mobile Device Management (MDM):**
  Implementieren Sie MDM-Lösungen, um die Sicherheit und Verwaltung der Geräte zu gewährleisten.

Authentifizierung versus Authentisierung

Ein häufiges Missverständnis besteht in der Verwendung der Begriffe „Authentifizierung“ und „Authentisierung“. Authentifizierung bezieht sich auf den Prozess der Überprüfung der Identität eines Benutzers. Authentisierung hingegen ist der Nachweis, dass eine Identität tatsächlich diejenige ist, die sie vorgibt zu sein. Im Kontext der 2FA ist der korrekte Begriff „Authentifizierung“, wenn es darum geht, die Identität des Benutzers zu überprüfen.

2FA überall anwenden

Es ist entscheidend, die Zwei-Faktor-Authentifizierung überall dort anzuwenden, wo es möglich ist. Ob bei der Anmeldung zu E-Mail-Konten, sozialen Netzwerken oder bei der Nutzung von Cloud-Diensten – die zusätzliche Sicherheitsebene der 2FA kann einen erheblichen Unterschied machen. Durch die breite Anwendung von 2FA können wir die Risiken von Datenverlust oder -diebstahl erheblich minimieren und unsere digitalen Identitäten besser schützen.

Unsere Verpflichtung zur Sicherheit

Bei der Zusammenarbeit mit unseren Kundinnen und Kunden setzen wir als Kommunal Agentur NRW konsequent die oben genannten Methoden zur Authentifizierung ein. Unsere Mitarbeitenden achten bei der täglichen Zusammenarbeit darauf, dass die erforderlichen Sicherheitsstandards eingehalten werden.

Wir legen großen Wert darauf, dass alle Sicherheitsmaßnahmen stets dem Stand der Technik entsprechen. Dazu gehören biometrische Verfahren wie Fingerabdruck- und Gesichtserkennung, Hardware-gestützte Authentifizierungsmethoden wie Sicherheits-Token und USB-Schlüssel sowie moderne Ansätze wie Push-Benachrichtigungen und adaptive Authentifizierung.

Durch die Integration dieser Methoden in unsere Mobile-Device-Management-(MDM-)Lösungen stellen wir sicher, dass alle mobilen Geräte, die für dienstliche Zwecke genutzt werden, optimal geschützt sind. Unsere Mitarbeitenden sind geschult, diese Technologien effektiv einzusetzen und kontinuierlich zu überwachen, um die Sicherheit unserer Daten und die unserer Kunden und Kundinnen zu gewährleisten.

Wir sind uns der Verantwortung bewusst, die mit dem Schutz sensibler Daten einhergeht, und setzen alles daran, diese Verantwortung ernst zu nehmen. Durch die konsequente Anwendung der beschriebenen Authentifizierungsmethoden können wir das Risiko von Datenverlust oder -diebstahl minimieren und ein Höchstmaß an Sicherheit bieten.

Fazit

Die Zwei-Faktor-Authentifizierung ist ein unverzichtbares Werkzeug, um die Sicherheit sowohl persönlicher als auch dienstlicher Daten zu erhöhen. Besonders in einer Zeit, in der mobile Geräte eine zentrale Rolle in unserem Arbeitsalltag spielen, ist es wichtig, diese zusätzlichen Sicherheitsmaßnahmen zu ergreifen. Durch die richtige Implementierung und Nutzung von 2FA können wir unsere Daten effektiv schützen und die Risiken von Datenverlust oder -diebstahl minimieren.

*Mit Ihren Anliegen zur Datensicherheit sind Sie bei **Karsten Klick** genau richtig. Er leitet bei der Kommunal Agentur NRW den Sachbereich Informationstechnologie.*

Telefon 0211 430 77 107
klick@KommunalAgentur.NRW