nevisIDM – Unterstützung von Google Authenticator mit OATH

Vorteile

Mit Google Authenticator, Authy, FreeOTP und anderen OATH-Smartphone-Apps können Benutzer **mit wenig Zusatzaufwand starke Authentisierung nutzen** – ein Smartphone ist alles, was es dazu braucht.

Starke Zwei-Faktor-Authentisierung mit nevisIDM und OATH **verringert das Risiko und die Auswirkungen von Identitätsdiebstahl**. Die für den Authentisierungsprozess verwendeten Einmalpasswörter (One-time Passwords, OTPs) sind nur einmal gültig. Angreifer könnten mit den Login-Daten, selbst wenn sie sie stehlen könnten, also nichts anfangen.

Worum geht es?

Ihre Anwendungen sind wertvoll. Der sichere Zugriff auf diese Anwendungen ist entscheidend und muss durch zuverlässige Authentisierungsverfahren geschützt werden.

Üblicherweise werden zum Beispiel Passwörter und Sicherheitsfragen für die Authentisierung verwendet. Leider sind die betreffenden Verfahren nicht sicher. Sobald ein Angreifer das Passwort oder die Antwort auf die Sicherheitsfrage kennt, kann er direkt auf das System zugreifen.

Mit starken Authentisierung ist ein derartiger böswilliger Zugriff wesentlich schwieriger. OATH, die „Initative for Open Authentication", fördert die Verwendung sicherer Authentisierungsoptionen.

nevisIDM unterstützt zwei OATH-Algorithmen: HOTP und TOTP. Ein HOTP ist ein „HMAC-based One-Time Password" (HMAC-basiertes Einmalpasswort). HMAC steht für „Keyed-Hash Message Authentication Code". HOTPs sind ereignisgesteuert, werden also nur auf Anforderung (z. B. beim Klicken auf eine Schaltfläche) erzeugt. Auch TOTPs sind Einmalpasswörter, in diesem Fall jedoch zeitgesteuert. Diese Passwörter sind jeweils nur eine bestimmte Zeit lang gültig.

In Verbindung mit einer OATH-App wie Google Authenticator können Sie sich damit mit sicherer Zwei-Faktor-OATH-Authentisierung in Ihre Anwendungen einloggen.
Die Zwei-Faktor-Authentisierung erfordert jeweils einen Nachweis aus zweien der drei folgenden Kategorien: etwas, das Sie wissen; etwas, das Ihnen gehört; etwas, das Sie sind. Etwas, das Sie wissen, könnte ein Passwort oder eine PIN sein. Etwas, das Ihnen gehört, könnte eine Rasterkarte oder ein Token eines Dritten sein. Etwas, das Sie sind, bezieht sich auf biometrische Parameter. Es könnte sich um einen Fingerabdruck, Ihre Stimme, Ihre Schreibgewohnheiten usw. handeln.

Mit OATH-Authentisierung lässt sich die Kategorie „etwas, das Ihnen gehört", wesentlich einfacher bedienen. Ihr Smartphone ist etwas, das Ihnen gehört, und hat zusätzlich den Vorteil, dass Sie es höchstwahrscheinlich ohnehin immer dabei haben.

Die Vorgehensweise ist einfach. Laden Sie zunächst eine OATH-App herunter (z. B. Google Authenticator). Aktivieren Sie dann die Zwei-Faktor-Authentisierung, indem Sie den auf dem Bildschirm angezeigten QR-Code scannen.

Von nun an wird bei jedem Login in Ihre NEVIS-geschützte Anwendung neben den normalen Login-Daten (z. B. Benutzername und Passwort) auch ein OTP abgefragt. Das OTP kann auch ohne Internetzugang erzeugt werden. Ausserdem wechselt es oft, da es im Fall eines TOTP automatisch und im Fall eines HOTP auf Anfrage neu erzeugt wird. Das bedeutet, dass Angreifer, selbst wenn ihnen der Diebstahl Ihrer Login-Daten gelingt, nichts mit diesen Daten anfangen können, da sie nicht mehrmals verwendet werden können.

Wichtigste Merkmale

- Starke Zwei-Faktor-Authentisierung mit wenig zusätzlichem Aufwand.
- Zugriff auf alle Ihre Anwendungen mit Google Authenticator, Authy, FreeOTP und anderen Authentisierungs-Apps.
- Automatische Neuerzeugung von Passwörtern.
- Einmal-Passwörter.
- Kein eigenes Gerät für starke Authentisierung erforderlich – Smartphone reicht aus.
- Wahlweise zeitgesteuertes Einmalpasswort (TOTP) oder HMAC-basiertes Einmalpasswort (HOTP).

Schweiz ▪ AdNovum Informatik AG ▪ Röntgenstrasse 22 ▪ 8005 Zürich ▪ Schweiz ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapur ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Deutschland ▪ NEVIS Security GmbH ▪ Maximilianstraße 35 A ▪ 80539 München ▪ Deutschland ▪ +49 89 2421 8180 ▪ info@nevis-security.de ▪ www.nevis-security.de

Vorgehensweise beim Einrichten

Ein Benutzer möchte auf eine Anwendung (Zielanwendung) zugreifen, hat aber noch nie mit OATH-Authentisierung gearbeitet. Das Mobiltelefon des Benutzers und nevisIDM besitzen also noch keinen geheimen Schlüssel, der für die Erzeugung eines OTP erforderlich ist.

Um die Zwei-Faktor-Authentisierung einzurichten, muss der Benutzer bereits authentisiert sein, z. B. mittels der Kombination aus Benutzername und Passwort (1). Der Server erzeugt dann einen geheimen Schlüssel, der dem Benutzer als QR-Code angezeigt wird (2). Der Benutzer scannt/gibt den geheimen Schlüssel mit der OATH-App (z. B. Google Authenticator) auf seinem Mobiltelefon ein (3). Die OATH-App und nevisIDM kennen nun beide den geheimen Schlüssel (4).

Optional kann der Benutzer testen, ob der geheime Schlüssel ordnungsgemäss importiert wurde. Dazu gibt er im Browser ein Einmalpasswort ein (6), das mit der OATH-App erzeugt wurde (5). Wurde das OTP richtig eingegeben, hat der Benutzer die Zwei-Faktor-Authentisierung erfolgreich aktiviert und kann diese nun verwenden.

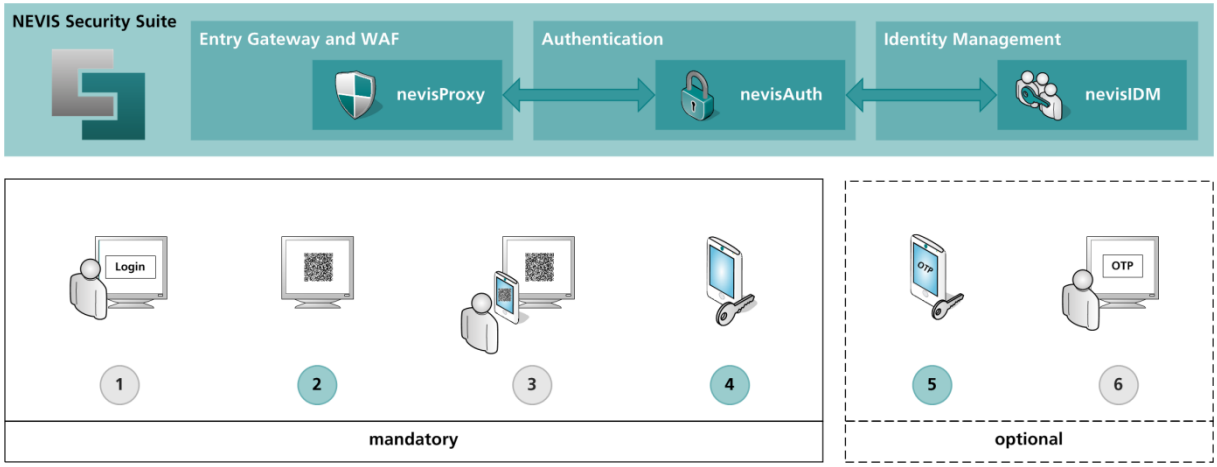

Abbildung 1 Vorgang beim Einrichten

Vorgehensweise beim Einloggen

Der Benutzer fordert im Browser Zugriff auf seine Zielanwendung an (1). nevisProxy und nevisAuth kommunizieren und fragen den Benutzer nach seinen Login-Daten, z. B. nach seinem Benutzernamen und Passwort (2). Nach Eingabe der richtigen Informationen fragt nevisAuth nach dem OTP (3). Der Benutzer ruft auf seinem Mobiltelefon die OATH-App auf (z. B. Google Authenticator), die unter Verwendung des bei der Einrichtung erzeugten geheimen Schlüssels ein OTP erzeugt (4). Der Benutzer gibt dieses OTP im Browser ein (5). nevisIDM prüft das OTP und leitet den Benutzer bei erfolgreicher Prüfung an seine Zielanwendung weiter (6).

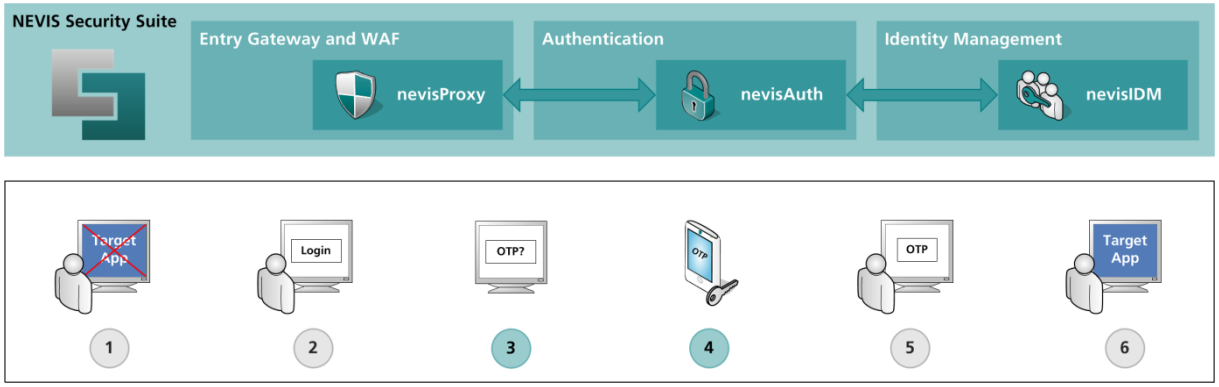

Abbildung 2 Login-Vorgang

Schweiz ▪ AdNovum Informatik AG ▪ Röntgenstrasse 22 ▪ 8005 Zürich ▪ Schweiz ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapur ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Deutschland ▪ NEVIS Security GmbH ▪ Maximilianstraße 35 A ▪ 80539 München ▪ Deutschland ▪ +49 89 2421 8180 ▪ info@nevis-security.de ▪ www.nevis-security.de