

## Verschärfte Bedrohungslage: phishing-resistente Anmeldung für privilegierte Zugriffe

Passwortlos mit Passkeys und FIDO2 – wie wir den administrativen Zugang zu Ihren Cloud-Systemen absichern und was das für Sie bedeutet.

Die Bedrohungslage verschärft sich: KI-gestützte Phishing-Kampagnen treffen Unternehmen heute teils gezielt, teils breit gestreut. Wir sehen aktuell sehr häufig gefälschte SMS- und Einmalcode-Nachrichten, die für Anwender nicht mehr von echten zu unterscheiden sind – klassische Verfahren wie SMS-Codes oder App-Bestätigungen bieten hier keinen verlässlichen Schutz mehr. Deshalb legen wir bei modernX die Messlatte höher: Jeden privilegierten Zugriff auf Ihre und unsere Systeme haben wir auf eine phishing-resistente, passwortlose Multifaktor-Authentifizierung umgestellt. So ist der administrative Zugang zu Ihren Cloud-Systemen jederzeit nach dem Stand der Technik geschützt.

**Warum gerade jetzt?** KI-Modelle von OpenAI haben laut aktuellen Berichten einen Cyberangriff auf die KI-Plattform Hugging Face autonom ausgeführt – ohne menschliches Zutun ([tagesschau.de](https://www.tagesschau.de), [heise.de](https://www.heise.de)). Jeder Tag mit Passwort und SMS-Code ist ein Tag Vorsprung für die Angreifer.

### Was ist ein Passkey bzw. ein FIDO2-Sicherheitsschlüssel?

Ein Passkey ersetzt das Passwort durch ein kryptografisches Schlüsselpaar: Der private Schlüssel verlässt nie das Gerät – etwa einen Hardware-Sicherheitsschlüssel nach dem FIDO2-Standard. Die Anmeldung funktioniert zudem nur bei der echten Domain; eine nachgebaute Login-Seite läuft ins Leere. Es gibt schlicht kein Passwort und keinen Code mehr, den ein Angreifer stehlen oder abfragen könnte.

**0 %** erfolgreiche Kontoübernahmen bei Hardware-Sicherheitsschlüsseln – in einer Google-Studie mit 350.000 realen Angriffsversuchen. SMS-Codes stoppten nur 76 % der gezielten Angriffe.

## Ihre Sicherheit liegt uns am Herzen

### Kostenfrei für Sie

#### Privilegierte Zugriffe: bereits umgestellt

Sämtliche Zugriffsmöglichkeiten unserer Benutzer auf Ihre Umgebung haben wir auf das sichere Verfahren umgestellt – passwortlos und phishing-resistent. Sie erhalten dazu eine kurze Information; wo die Umstellung noch aussteht, kommen wir aktiv auf Sie zu.

### Kostenfrei für Sie

#### Entra-Kennwortschutz: für Sie umgesetzt

Den Microsoft Entra-Kennwortschutz haben wir für Ihre und unsere Cloud-Identitäten umgesetzt, die noch nicht per Passkey oder FIDO2 geschützt sind. Schwache und kompromittierte Passwörter werden gar nicht erst zugelassen – mit wenig Aufwand auf Ihr lokales Active Directory ausweitbar, je nach Lizenzierung ergänzt um Microsoft Defender for Identity.

### Wir gehen weiter

#### Jetzt auch Ihre Benutzer umstellen

Wir empfehlen dringend, auch Ihre Benutzer auf das neue Verfahren umzustellen – und unterstützen Sie gerne dabei. Wir kommen dazu in Kürze auf Sie zu. Sie möchten nicht warten? Rufen Sie uns an oder schreiben Sie an [willkommen@modernx.de](mailto:willkommen@modernx.de).

## Passkey per Smartphone – oder als Hardware-Schlüssel

Die Anmeldung per Passkey funktioniert auch rein über Ihr Smartphone: wie gewohnt, nur deutlich sicherer. Sie wollen noch mehr? Dann sind Hardware-Schlüssel ideal. FIDO2-Sicherheitsschlüssel wie den [YubiKey 5C NFC](#) erhalten Sie auf Wunsch auch über uns als Service\* – inklusive Beschaffung, Austausch und Ersatzschlüsseln, ohne einmalige Großinvestition. Auf Wunsch auch als FIPS-140-3-Variante, dem aktuell höchsten Zertifizierungsstandard für kryptografische Module.

\* ab 100 Stück, Details unter [yubico.com/resource/yubikey-as-a-service](https://yubico.com/resource/yubikey-as-a-service)

Gerne beraten wir Sie zu diesem Thema – sprechen Sie uns an oder vereinbaren Sie direkt einen Termin.