BERGT • working it-services • Kantstr. 53 • 14612 Falkensee

Multi-Faktor-Authentifizierung für Ihre ständig wechselnden Anforderungen

Erweiterte Authentifizierung

Wenn Sie Zeit, Ressourcen und Budget in eine Multi-Faktor- oder Zwei-Faktor-Lösung investieren, möchten Sie dadurch möglicherweise eine konkrete Herausforderung bewältigen. Punktlösungen können häufig genau das und sind nicht flexibel genug, um auch zukünftigen Herausforderungen zu begegnen. Aber Sie können versichert sein, dass es einen besseren Weg gibt. NetIQs intelligente, flexible Multi-Faktor-Authentifizierungslösung wurde entwickelt, um den Herausforderungen von heute ebenso gerecht zu werden wie den sich ständig ändernden Anforderungen von morgen.

Produktübersicht

Ein Framework für jede Authentifizierung

Unternehmen müssen in der Regel mehrere Infrastrukturen verwalten und betreuen. Dies ist nicht nur kompliziert, sondern bietet auch nur eine eingeschränkte Sicherheit. Was Sie benötigen, ist ein einziges Authentifizierungs-Framework für all Ihre Geräte und Methoden. Mit einem einzigen Framework lassen sich Kosten geringhalten, da Advanced Authentication sich an Umgebungen jeder Größe anpassen lässt.

Der Benutzerverifizierung gerecht werdende Authentifizierung

Jedes Unternehmen verfügt über vertrauliche Informationen (Finanzdaten, Kundendaten, vertrauliche Daten usw.), die eine zusätzliche, mit herkömmlichen Zugangsdaten nicht zu realisierende Benutzerüberprüfung erforderlich machen. Diese Art von Informationen rechtfertigt je nach Situation einen höheren Grad an Authentifizierung. Befindet sich der Anfordernde wie erwartet im Gebäude, an einem anderen Ort im Inland oder außerhalb der Landesgrenzen? Verwendet er oder sie ein bekanntes Gerät oder ein bisher unbekanntes? Vielleicht gibt es andere Kriterien, anhand derer Sie die Authentifizierungsstufe steuern möchten. NetIQ bietet eine risikobasierte Zugriffskontrolle, mit deren Hilfe Sie die Art der Authentifizierung an das potenzielle Risiko des Zugriffs auf die Informationen oder den Dienst anpassen können.

NetIQ gibt Ihnen die Freiheit den Authentifizierungstypen zu verwenden, der Ihrem Unternehmen am besten passt.

Unterstützung mobiler Mitarbeiter – Offlineanmeldung

Mitarbeiter können nun jederzeit von unterwegs aus eine Multi-Faktor-Authentifizierung für den Zugriff auf private Daten durchführen. Dies bedeutet, dass Benutzer auch ohne Konnektivität Aufgaben erledigen können.

Unterstützung für mehrere Standorte

Große Unternehmen, die ihre Authentifizierungsrichtlinien weltweit implementieren müssen, können davon profitieren, dass Advanced Authentication eine Konfiguration für mehrere Standorte unterstützt. Advanced Authentication wurde dazu entwickelt, all Ihre Anforderungen in Bezug auf Leistung und Standort zu erfüllen.

Lösung

Security & Identity

Produkt

Advanced Authentication

Funktionen:

Unterstützung zahlreicher Plattformen

Hohe Verfügbarkeit: Redundanz und Lastausgleich

Geo-Fencing

Unterstützung für mehrere Standorte

Advanced Authentication für Active Directory Federation Services (ADFS)

Integrierter FIPS 140-2

Webbasierte Benutzerregistrierung

Unterstützung mobiler Mitarbeiter

Unterstützung zahlreicher Plattformen

NetIQ unterstützt Sie bei der Gewährleistung der IT-Sicherheit Ihrer unterschiedlichen Plattformen. Von daher bietet Advanced Authentication ein Plugin für die Authentifizierung für OS X sowie ein Authentifizierungsmodul für Linux. Dies ergänzt den bereits vorhandenen Windows Credential Provider. Sie können auf iOS, Android und Windows Mobile basierende Methoden für die Authentifizierung von Windows 7+ und OS X 10+ Computern für geschäftskritische Initiativen nutzen. Durch die Unterstützung zahlreicher Plattformen können Sie eine umfassende Abdeckung beschleunigen und die entstandenen Kosten senken, wenn ansonsten mehrere Lösungen erforderlich waren.

Hohe Verfügbarkeit: Redundanz und Lastausgleich

Advanced Authentication zeichnet sich durch eine hohe Verfügbarkeit aus und ermöglicht einen kontinuierlichen, unterbrechungsfreien Betrieb. Anwendungsverfügbarkeit, Zuverlässigkeit und Leistung werden durch interne Server-Lastausgleichsfunktionen gewährleistet. Zugleich sichert die Reproduktion zwischen einem primären Standort und sekundären Standorten (über LAN oder WAN) die Datenintegrität. Mehrere aktualisierte Datenspeicher sind für ein schnelles Disaster Recovery (DR) stets verfügbar.

Integrierter FIPS 140-2

Da die Verschlüsselungsnormen des National Institute of Standards and Technology (NIST) weltweit anerkannt sind, ist die Norm FIPS 140-2 (Federal Information Processing Standard) für jedes Unternehmen von Bedeutung. Advanced Authentication erfüllt diese Normen, weshalb es von sicherheitsbewussten Unternehmen sowie Organisationen in regulierten Branchen problemlos implementiert werden kann.

Webbasierte Benutzerregistrierung

Advanced Authentication bietet einen einfachen selbsterklärenden Ablauf für die Endbenutzerregistrierung. Dank einer vereinfachten Registrierung von iOS-, Android- und Windows Phone-Geräten sowie Workstation-gebundener Biometrie, Kartenlesefunktionen etc. registrieren Ihre Benutzer Ihre Geräte wirksam, Ihr System ist einfach zu skalieren und Ihr Helpdesk wird nicht mit Anrufen wegen Komplikationen bei der Registrierung überlastet.

Helpdesk-Modul

Das Helpdesk-Modul bietet die nötigen Funktionen, um eine durchgängig gute Benutzererfahrung zu gewährleisten. Dazu gehören die Deregistrierung und die Unterstützung bei Methoden für die erneute Registrierung, die Zuweisung von Token (bei Bedarf) sowie die Zuweisung bestimmter Benutzerrollen. Wenn ein Benutzer sich mit einem Authentifizierungsproblem im Zusammenhang mit Advance Authentication an den Helpdesk wendet, kann Ihr Helpdesk-Mitarbeiter dem Kunden die erwartete positive Kundensupport-Erfahrung bereitstellen. Dadurch entstehen enge Beziehungen und eine weitere Unterstützung Ihrer MFA (Multi-Faktor-Authentifizierung).

Notfall-Einmalkennwort (One-Time Password, OTP)

Nutzen Sie diese Funktion von Advanced Authentication, wenn einem Benutzer keine zuvor registrierte Authentifizierungsmethode zur Verfügung steht. Möglicherweise hat Ihr Benutzer seinen Token verlegt, ist mit seinem Telefon baden gegangen oder befindet sich einfach an einer Workstation, bei der das Kartenlesegerät ausgefallen ist. In jedem Fall braucht er trotzdem Zugriff. Der Notfall-Zugriff per OTP ist Teil des Helpdesk-Moduls und ermöglicht in solchen dringenden Situationen die Erstellung eines Einmalkennworts für den Benutzer.