indevis
Sicherheit in einer vernetzten Welt

Ihre Vorteile

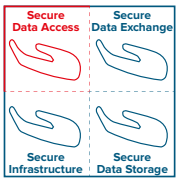
- Hochsichere Multi-Faktor Authentisierung (Hardware-Token, SMS-Token, Software-Token)
- Anbindung per VPN und AES-Verschlüsselung
- Hochverfügbarkeit durch redundante Auslagerung in professionelle Rechenzentren
- Optional virtuelles System mit eigener Administrationsoberfläche
- Rundum-Service durch indevis: Setup und Design, Token-Rollout, Replacement Service, Service Desk
- Skalierbare Kosten; Investitions-Verschiebung von Capex zu Opex

cloud services
MADE IN GERMANY

SIE WOLLEN
MEHR ERFAHREN?

Ihr persönlicher Ansprechpartner berät Sie gerne und findet mit Ihnen heraus, welches Konzept am besten zu Ihnen passt.

+49 (89) 45 24 24-100
sales@indevis.de
www.indevis.de



INDEVIS AUTHENTICATION

STARKE AUTHENTIFIZIERUNG FÜR JEDE ORGANISATIONSGRÖSSE

Statische Passwörter (Benutzername und Passwort) bieten keine ausreichende Sicherheit, um das Netzwerk vor ungewollten Zugriffen zu schützen. Oft ist ein Passwort sehr einfach zu erraten oder gelangt in unberechtigte Hände. Auch das Ausspionieren statischer Passwörter ist mit den heutigen Mitteln der Technik kein Problem mehr. Spezielle Tools probieren automatisiert mehrere Millionen Wortkombinationen in kürzester Zeit. Wenn Passwörter über das Internet übertragen werden, können potenzielle Angreifer diese oft ohne große Mühe erlangen.

DER ENTSCHEIDENDE FAKTOR FÜR MEHR SICHERHEIT

Eine Zwei-Faktor-Authentifizierung mit einem zusätzlichen (Hardware-) Token ist die optimale Lösung für einen abgesicherten Netzwerkzugang. Dabei erfolgt die Anmeldung an den Unternehmenssystemen nicht über ein statisches Passwort, sondern über eine Kombination aus einer PIN (1. Faktor) und einem sich laufend ändernden Code, der auf einem separaten Gerät angezeigt oder per SMS zugeschickt wird (2. Faktor). Mit einer solchen starken und benutzer-freundlichen Authentifizierung lässt sich eine einfache aber trotzdem sehr sichere Netzwerkanmeldung realisieren – für Verwaltung, Geschäftsleitung, Administration, Vertrieb, Kunden, externe Dienstleister etc.

LANGJÄHRIG UND VIELFACH BEWÄHRTE TECHNOLOGIE

indevis Authentication bietet Unternehmen und Organisationen jeder Größenordnung auf der Basis von RSA SecurID ein Benutzer-Authentifizierungssystem mit dynamischen Passwörtern. indevis betreibt schon seit 1999 einen RSA Authentifizierungsserver in einem speziell gesicherten Rechenzentrum einer Großbank – mittlerweile besteht Hochverfügbarkeit der Infrastruktur durch ein redundantes zweites Rechenzentrum. Viele Tausend Token der *indevis Authentication* Lösung wurden seit diesem Zeitpunkt ausgerollt und schützen bis heute Unternehmensressourcen von unschätzbarem Wert.

SKALIERBARE LÖSUNG – MAXIMALER NUTZEN

indevis Authentication ist ein perfekt skalierbares Mietmodell und schon für minimale Kosten pro Monat verfügbar. Ihr Unternehmen mietet für eine monatliche Pauschale genau so viele Token, wie Sie in Ihrer Organisation benötigen – für jeden neuen Mitarbeiter können Sie einzelne Token anmieten. Dadurch lassen sich die Total Costs of Ownership drastisch reduzieren und Ihr Unternehmen nutzt sofort eine voll funktionsfähige RSA SecurID Authentifizierung ohne große Anfangsinvestition.

indevis Authentication Services:

- indevis betreibt und administriert den RSA ACE/Server
- indevis administriert die RSA SecurID Benutzerverwaltung
- indevis übernimmt den Token-Rollout in Ihrem Unternehmen
- indevis ersetzt alte und verlorene Token

FUNKTIONSWEISE INDEVIS AUTHENTICATION

Bei der Authentifizierung mit RSA SecurID muss der Benutzer bei der Anmeldung an einer Netzwerkressource seinen Benutzernamen, seine selbst gewählte PIN und den Tokencode eingeben. Als Authentisierungs-Token können sowohl ein Hardware-Token, ein SMS-Tokencode, als auch ein Software-Token verwendet werden.

Die eingegebenen Daten werden über den RSA Agent übermittelt, welcher die Authentifizierungsanfrage verschlüsselt und sie an den von indevis betriebenen RSA Authentication Manager Server zur Überprüfung der Authentizität des Benutzers weiterleitet. Der RSA Authentication Manager errechnet anhand Uhrzeit und Startwert den aktuell gültigen Zugangscode und übermittelt das Authentifizierungsergebnis an den entsprechenden RSA Agent zurück. Bei Übereinstimmung der Daten ist die Authentifizierung erfolgreich und der RSA Agent gestattet (oder verweigert) dem Anwender den Zugriff auf die Netzwerkressourcen.

ANBINDUNG PER VPN UND AES-VERSCHLÜSSELUNG

indevis Authentication ist für die meisten Unternehmen die günstigste Variante, ihre statischen Passwörter durch dynamische abzulösen. Das Kunden-LAN wird dabei über VPN an den indevis Authentifizierungsserver angebunden. Die Authentifizierung erfolgt AES-verschlüsselt durch das Internet. Dabei werden keine Unternehmensdaten an den indevis RSA Authentication Manager übermittelt. Lediglich Tokencode, PIN, Benutzername und RSA Agent-Name werden übertragen.

SOFTWARE-TOKEN: ERLEICHTERTE AUTHENTIFIZIERUNG UND VERTEILUNG MITTELS QR-CODE

Durch den Einsatz von Software-Token kann der Workflow für die Verteilung und das Management der Zwei-Faktor-Authentifizierung für weltweite mobile Mitarbeiter optimiert werden. Der Token Seed – der geheime Schlüssel, der das Passwort erzeugt – kann dem Nutzer als QR-Code postalisch übersendet werden. Dies erleichtert die Verteilung der Token besonders für Firmen, die global agieren. Beim Versand des QR-Codes als Brief müssen keine Import- oder Zollbestimmungen beachtet werden, sodass der Token schnell ankommt. Der Verteilweg selbst ist außerdem sicherer als der Versand über unverschlüsselte E-Mails, da er Hackerangriffe unmöglich macht.

Für Nutzer bietet der Software-Token die Vorteile, dass er nutzerfreundlich, auf dem Smartphone immer griffbereit und leicht in Betrieb zu nehmen ist. Denn der QR-Code führt automatisch zur RSA-App, sobald der Nutzer ihn mit seinem Smartphone abfotografiert. Zum Aktivieren des Tokens erhalten die Mitarbeiter separat ein Passwort mit einem zweiten Brief per Post. Die Bedienung über die App ist einfach, da lediglich der persönliche Pin eingegeben werden muss und sich der Passcode aus diesem und dem Token Code automatisch errechnet.

Sie wollen *indevis Authentication* kennenlernen? Auf Wunsch stellen wir Ihnen eine kostenlose Teststellung zur Verfügung – und Sie erhalten sofort einen flexiblen und sicheren Remote Access für Ihr Unternehmen.

Über die indevis GmbH

Die ISO 27001 zertifizierte indevis GmbH bietet seit 1999 IT-Sicherheits-, Datacenter- und Netzwerklösungen, flankiert von professionellen Consulting-, Management- und Support-Dienstleistungen. Dabei erfüllt indevis sowohl die Anforderungen der Wirtschaft als auch die von öffentlichen Behörden und Hochschulen.

Als einer von Deutschlands führenden Managed Security Service Providern ist indevis der Partner für IT-Sicherheit und Netzwerktechnik für Unternehmen jeder Größe und Branche – denn IT Sicherheit passiert nicht von alleine, sondern muss strategisch geplant werden.

indevis betreibt zwei Niederlassungen: in München und Hamburg. Weitere Mitarbeiter agieren von mehreren Standorten über Deutschland verteilt aus.

TÜV SÜD ISO 27001

indevis
Sicherheit in einer vernetzten Welt

indevis GmbH

Irschenhauser Straße 10
81379 München

Tel. +49 (89) 45 24 24-100
Fax: +49 (89) 45 24 24-199

sales@indevis.de
www.indevis.de