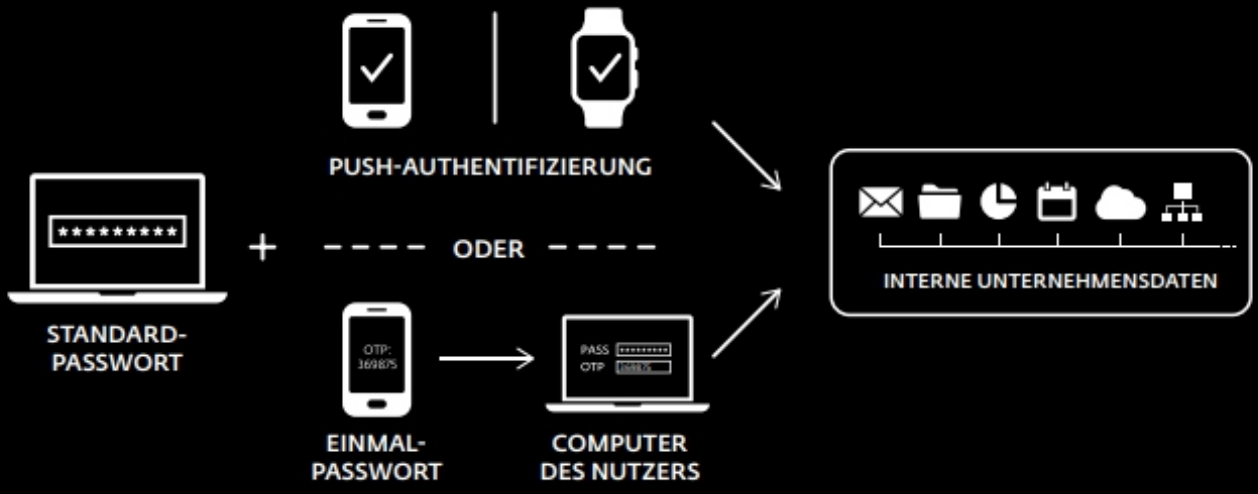
2 Faktor Authentifizierung

Zusätzliche Anmeldebestätigung mit Handy App



Sind Sie sicher, dass sich nur die Benutzer an Ihrem Server anmelden, denen Sie Benutzernamen und Kennwort übergeben haben?

Sind Sie sicher, dass Ihr Mitarbeiter Ihr Firmenkennwort nicht auch bei unsicheren Webdiensten als Kennwort benutzt oder sein Kennwort durch Phishing Attacken abgegriffen wurde?

Dass der Zugriff auf Ihre Server nur vom gewünschten Mitarbeiter stattfinden kann, könnte mit unserer 2 Faktor Authentifizierung sichergestellt werden, da der Zugang von extern zusätzlich am Handy des Mitarbeiters bestätigt werden muss. Und falls das Handy gestohlen wurde fällt sowas ganz schnell auf!

Sie sind dies schon beim Onlinebanking gewohnt, auch da ist die 2 Faktor Authentifizierung Pflicht, nun können wir das auch für Ihre Server anbieten.

ERHÖHEN SIE DEN ZUGRIFFSCHUTZ AUF IHRE DATEN !

Benutzername und Kennwort reichen in der heutigen Zeit nicht mehr aus um sicher zu überprüfen wer auf Ihre Daten zugreifen kann! Überprüfen Sie zusätzlich den Zugriff auf Ihre IT durch die Bestätigung auf dem Smartphone Ihres Mitarbeiters.

Bei der Zwei-Faktor-Authentifizierung wird Ihr PC/Terminalserver nicht nur durch Ihren Benutzernamen und Kennwort gesichert, sondern durch eine weitere Abfrage auf Ihrem Handy oder Ihrer Smartwatch.
Die 2FA macht Ihren Account somit wesentlich sicherer. Sollte es Hackern gelingen, an Ihre Login-Daten zu kommen, benötigen diese ebenfalls Ihr Smartphone, um den Zugriff zu erhalten!

Ihre Passwörter können gehackt werden. Selbst das stärkste Passwort hilft da nichts wenn andere Ihre Kennworteingabe filmen und nachvollziehen, es geknackt oder auf unsicheren Servern gespeichert wurde.
Die 2FA stellt hier eine weitere Hürde für Hacker dar. Dies kann die einfache Bestätigung sein, Ihr Fingerabdruck auf dem Handy oder falls Sie aktuell mit dem Handy keine Internetverbindung haben, kann auch mit der Handy-App ein Einmal-Kennwort erzeugt werden.
Eindringlinge müssen also zusätzlich zum Kennwort auch noch Zugriff auf Ihr Handy haben! Ihre Zugänge sind mit unserer Zwei-Faktor Authentifizierung daher deutlich besser geschützt.

Bei mehr als 80% der weltweiten Cyberangriffe wurden unsichere Passwortverfahren ausgenutzt. Passwörter allein reichen also nicht mehr aus. Jeden Tag verwenden Cyberkriminelle gestohlene Anmeldedaten, um auf Systeme zuzugreifen, diese zu infizieren oder Daten zu stehlen.
Nicht umsonst enthalten viele gesetzliche Vorgaben die Pflicht zu MultiFaktor-Authentifizierung. Die meisten Datenlecks werden durch gestohlene oder schwache Passwörter verursacht.

net-solution
Ihr Cloud Service Provider

Beindstr. 12
68542 Heddesheim

06203 / 494949
Info@net-solution.net
www.net-solution.net

DREI GUTE GRÜNDE FÜR DIE ZWEI-FAKTOR-AUTHENTIFIZIERUNG

Unzureichende Kennwort Pflege
Häufig gelten Mitarbeiter als „größte Schwachstelle" der IT-Sicherheit eines Unternehmens.
Vor allem schlecht gepflegte Passwörter stellen eine große Gefahr fürs Business dar. Oft wird dasselbe Passwort für mehrere Anwendungen und Webseiten verwendet, notiert oder an Dritte weitergegeben. Klassische Gegenmaßnahmen wie die Pflicht, Passwörter regelmäßig zu ändern, bringen dabei oft wenig und führen noch mehr in Versuchung, ähnliche Passwörter zu verwenden oder Post-its mit den wichtigsten Kennwörtern an den Rechner zu kleben.
Eine Multi-Faktor-Authentifizierung schützt Unternehmen vor diesen Risiken, indem die reguläre Anmeldung um den zusätzlichen Faktor erweitert wird durch die Eingabe eines Einmal-Passworts, das auf dem Smartphone des Mitarbeiters generiert wird.
Damit schützen Sie sich vor Angreifern, die versuchen, durch einfaches Erraten schwacher Passwörter Zugang zu Ihren Systemen zu erlangen.

Datenschutzverletzungen
Beinahe täglich wird von Datenschutzverstößen in Unternehmen berichtet. Oft gelangen Angreifer über schwache oder gestohlene Zugangsdaten in das Unternehmensnetzwerk, die sie durch automatisierte Bots, Phishing oder zielgerichtete Angriffe ergattern. Über die Absicherung der normalen Logins hinaus kann die 2FA auch privilegierte Zugänge vor unautorisierten Zugriffen schützen. Mit einer 2 Faktor-Authentifizierung ist es für Angreifer wesentlich schwerer, Zugriff auf Ihre Systeme und Daten zu erlangen. In der Regel sind Unternehmen von Datenschutzvorfällen betroffen, die mit sensiblen Informationen arbeiten. Dazu gehört insbesondere die Finanzbranche, der Einzelhandel, das Gesundheitswesen und der öffentliche Sektor. Das heißt jedoch keineswegs, dass andere Branchen sicher sind. Wie jeder andere „Unternehmer" wägen professionelle Hacker Kosten und Nutzen eines Angriffs sorgfältig ab. Entsprechend sollte man es Ihnen so schwer wie möglich machen.

Compliance
Unternehmen müssen zunächst prüfen, ob sie Datenschutzvorgaben unterliegen oder nicht. Anschließend sollten sie ermitteln, welche Maßnahmen die Vorgaben empfehlen bzw. vorschreiben.
Eine starke Authentifizierung ist mittlerweile integraler Bestandteil gesetzlicher und anderer Vorgaben, darunter der EU-DSGVO. Vor allem Unternehmen, die mit Kreditkarteninformationen oder Gesundheitsdaten arbeiten, sind verpflichtet, den Schutz dieser Daten zu gewährleisten und entsprechende Maßnahmen vorzunehmen. Aber auch alle anderen Firmen sollten sorgfältig prüfen, ob bzw. an welche Datenschutzvorgaben sie gebunden sind.

KONFIGURATIONSMÖGLICHKEITEN

- Unsere Lösung wird von uns mit der zugehörigen Domäne (Active Directory) verknüpft, bei unseren Private Cloud Servern ist das schon aktiviert.
- Sie erfordert keine zusätzliche Hardware. Nach der Installation der Anwendung auf dem Server können wir umgehend mit der Bereitstellung starten.
- Wir können die Lösung bei all unseren Private Cloud Servern anbieten, aber auch falls Sie ein eigenes Domänennetzwerk in Ihrer Firma betreiben können wir dies konfigurieren.
- Ihre Mitarbeiter können bereits eingesetzte Smartphones weiter nutzen. Unsere 2FA ist für die Verwendung auf allen iOS und Android Smartphones geeignet. Für noch mehr Schutz und Bedienkomfort kann die App mit den Geräteeigenen biometrischen Verfahren (Touch ID, Face ID, Android Fingerprint) genutzt werden.
- PUSH-AUTHENTIFIZIERUNG: Bequeme Authentifizierung ohne Eingabe eines Einmal-Passworts über die Bestätigung einer Push-Benachrichtigung. Funktioniert auf iOS und Android Smartphones.
- Es müssen nicht alle Benutzer diese nutzen. Von Ihnen kann festgelegt werden, welche Benutzer 2FA benutzen sollen.
- Die Zwei-Faktor-Authentifizierung ist zwar sicher, kann jedoch bei häufigem Login ganz schön anstrengend werden. Wir können konfigurieren, dass bei Zugriffen aus Ihrem Büronetzwerk keine 2FA notwendig ist, bei Zugriffen von Extern oder einen Gatewayserver aber schon.
- Der Einloggvorgang pro Benutzer wird protokolliert.

Zusätzlicher Schutz beim Anmeldevorgang:
- Es kann der Zugriff auf Ihren Terminalserver /Sitzungshost geschützt werden.
- Es kann der VPN Verbindungsaufbau zu unseren Firewalls im Datacenter mit 2FA geschützt werden.
- Desktop-Logins und privilegierte Zugänge können ebenfalls durch die 2FA-Lösung geschützt werden. Wir unterstützen sowohl Windows als auch macOS und Linux.

PREISE
Bei unseren Private Cloud Servern ist dies schon vorkonfiguriert, betreiben Sie eine eigene Domäne oder eigene IT bei Ihnen vor Ort können wir die Voraussetzungen in ca. 1 Stunde installieren.

Monatliche Kosten pro aktiviertem Benutzer
(Es müssen nicht alle Mitarbeiter aktiviert werden!)

- bis zu 10 Benutzern: 3,00 EUR zzgl. MwSt.
- bis zu 25 Benutzern: 2,60 EUR zzgl. MwSt.
- bis zu 50 Benutzern: 2,20 EUR zzgl. MwSt.

net-solution
Ihr Cloud Service Provider
Beindstr. 12
68542 Heddesheim
06203 / 494949
Info@net-solution.net
www.net-solution.net