Besitz macht sicher(er)

Mehr Schutz für digitale Zugänge durch Zwei-Faktor-Authentisierung

Sicherheit bei der Anmeldung bedeutet meist Benutzername und Passwort. Doch das Verfahren ist fehleranfällig, umständlich und in die Jahre gekommen. Professionelle Anwender, beispielsweise von Virtual Private Networks (VPN), sollten auf jeden Fall zusätzliche Schutzmaßnahmen ergreifen. Zwei-Faktor-Authentisierung ist eine bewährte Ergänzung für unternehmenswichtige Zugangskontrollen. NCP bietet die Technik standardmäßig als Teil des Secure Enterprise Management-Servers an.

Wenn es um die Authentisierung von Zugängen geht, handelt ein großer Teil der Welt nach dem Motto „Never change a running system“. Weil Passwörter schon in den Zeiten vor Christus beschrieben wurden, müssen sie per Definition auch gut und sicher sein. Aber die aktuelle digitale Wirtschaft stellt andere Anforderungen an die Authentisierung als ein römisches Heereslager. Zum einen müssen sich aktuelle Benutzer weit mehr als ein Passwort merken. Ob PC, Tablet oder Smartphone, jeder Webdienst und jede Datenbank, verlangt nach einem – im besten Fall einzigartigen – Passwort. Zum anderen sind einfach zu merkende Klassiker wie „Flash“ (D-Day Kennwort der Alliierten) heute meistens nicht mal mehr erlaubt. Viele Webseiten stellen Mindestanforderungen an die Passwortgüte, unter sechs Zeichen Länge, einer Zahl und einem Sonderzeichen geht nichts mehr.

Mehr Schutz für unternehmenswichtige Dienste nötig

Wenn der eigene Account bei Labradorfreunde.de gehackt wird, ist das eine Sache. Wird aber der Zugang zum Firmennetz durch ein kompromittiertes Passwort offengelegt, sind die Folgen deutlich unangenehmer. Gerade VPNs sind darauf angewiesen, dass deren Nutzer eindeutig und fehlerfrei identifiziert werden können. Oft passiert dies ausschließlich durch Benutzernamen und Passwörter. Was dabei passieren kann, zeigten Mitte des Jahres die Vorkommnisse bei den Entwicklertools Mongo und CircleCI. Weil ein Anwender ein Passwort mehrfach verwendet hatte, konnte sich ein Angreifer damit beim VPN von Mongo anmelden und erhielt Zugriff zu Applikationen, mit denen er sukzessive seine Rechte weiter eskalieren konnte. Es ist praktisch unmöglich solche Versäumnisse und Pannen auszuschließen, selbst bei kleinen und mittelgroßen Firmen. Und wenn die Richtlinien für neue Passwörter zu streng gefasst werden, streiken die Anwender. Entweder weil sie sich nicht alle zwei Wochen ein neues, komplexes Passwort ausdenken und merken wollen, weil die Time-Out-Zeiten zu kurz sind oder weil die restriktiven Einstellungen auf Kosten der Produktivität gehen.

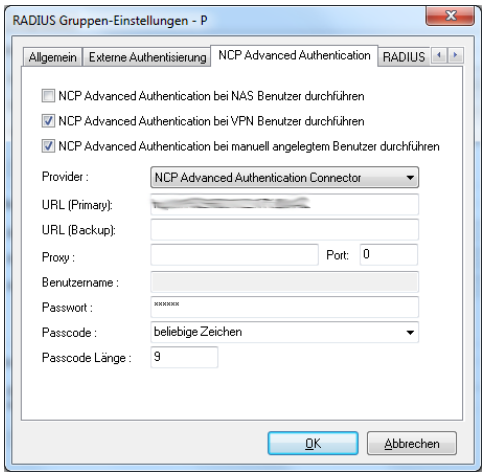
Dabei ginge es gerade im Firmenumfeld deutlich sicherer und einfacher. Zwei-Faktor-Authentisierung ist seit langer Zeit ein etabliertes Mittel, um zur wissensbasierten Authentisierung („Ich weiß mein Passwort“) noch einen besitzbasierten Faktor hinzuzufügen („Ich habe etwas, das ich zur Anmeldung benötige“). Mittlerweile beginnen viele populäre Web-Dienste, einen zweiten Faktor zur Sicherung ihrer Zugänge einzusetzen. So bieten Microsoft (OneDrive, Word.com, etc.) und Facebook diese

Möglichkeit, auch Dropbox lässt sich mit einem zweiten Anmeldefaktor absichern. Eine der interessantesten Ankündigungen zu diesem Thema gab Microsoft schon 2014 auf dem Entwicklerblog zu Windows 10 bekannt: Multi-Faktor-Authentisierung wird bei Windows 10 direkt integriert sein. Durch den standardmäßigen Einbau in das Betriebssystem wird die zusätzliche Sicherungsmethode für Anwender einfacher zu benutzen. Dahinter steckt die Hoffnung, dass sich die Nutzer über kurz oder lang von Passwörtern als der alleinigen Sicherungsmethode verabschieden werden.

Zahlreiche Spielarten der Zwei-Faktor-Authentisierung

Im professionellen Bereich wird die Zwei-Faktor-Authentisierung bei sicherheitskritischen Anwendungen wie VPNs schon lange als Option angeboten. Oft kommt dabei ein Token zum Einsatz, ein kleines Gerät mit Display, das zum Login-Vorgang eine Zahl anzeigt. Dieses One-Time-Passwort (OTP) muss der Benutzer zusätzlich zum Passwort eingeben. Token gelten als sehr sicher, sind aber kostspielig. Sie müssen konfiguriert, an die Benutzer verteilt und verwaltet werden. Token gehen verloren, werden gestohlen oder gehen kaputt – jedes Mal folgt ein administrativer Aufwand. Mittlerweile gibt es auch andere Ausführungen, die ohne Token auskommen. Die Bandbreite der Faktoren, die als zweites Authentisierungsmittel herangezogen werden können, reicht von einer SMS auf das Handy über eine E-Mail, ein durchgesagtes Kennwort per Telefonanruf, einen USB-Stick oder eine Smartcard bis hin zu einzigartigen technischen Merkmalen eines persönlichen Endgeräts des Anwenders.

NCP ermöglicht ab der Version 3.0 des VPN-Produkts Secure Enterprise Management (SEM) das OTP in Verbindung mit einem Handy oder Smartphone. Das Passwort wird über den NCP Advanced Authentication Connector oder einen SMS-Service-Provider auf das mobile Gerät des Nutzers übermittelt. Die starke Authentisierung via SMS bietet im Gegensatz zu Lösungen mit Hardware-Token den Vorteil, dass ein an den Anwender mitgeteiltes Einmalpasswort erst zum Zeitpunkt der Anmeldung zufällig generiert wird. Im Gegensatz dazu muss bei einer Token-basierten Lösung am Authentisierungsserver eine Tabelle vorgehalten werden, die zu jedem einzelnen Token in Abhängigkeit zur Uhrzeit das entsprechende Einmalpasswort enthält. Daraus ergibt sich ein potenzielles Risiko, sollte der Authentisierungsserver kompromittiert werden oder diese

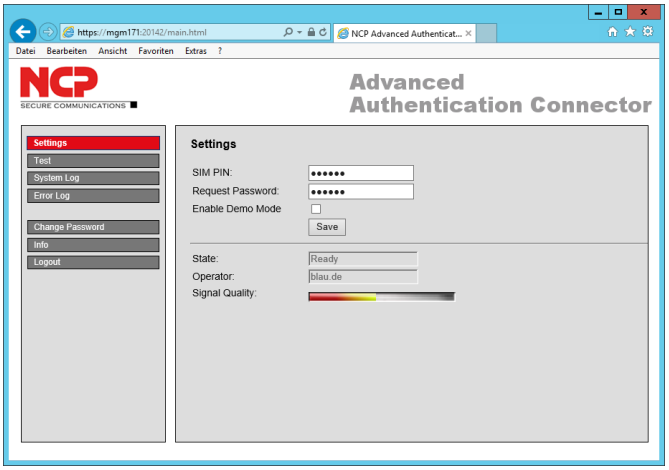


Nahtlos integriert:
Die Zwei-Faktor-Authentisierung ist standardmäßig Bestandteil von NCPs VPN-Lösung.

Tabelle in die falschen Hände geraten. Des Weiteren ergibt sich bei derartigen Lösungen der Nachteil, dass die verwendeten Hardware-Token nach einer gewissen Zeit ausgetauscht werden müssen, was zusätzliche Kosten verursacht. Für die Authentisierung via SMS genügt ein Mobiltelefon.

Optimal integrierte Zwei-Faktor-Lösung bei NCP

NCP bietet mit der Advanced Authentication zwei Varianten an, um SMS zu versenden. Für Installationen mit kleinen Benutzerzahlen kann der von NCP kostenlos bereitgestellte NCP Advanced Authentication Connector verwendet werden. Hierbei handelt es sich um eine Windows Software, die auf einem Rechner mit angeschlossener UMTS/GSM-Hardware installiert ist. Wird im Falle der Anmeldung eines Benutzers ein Einmalpasswort im NCP Secure Enterprise Management generiert, so wird dieses via sicherem HTTPS an den NCP Advanced Authentication Connector übermittelt und von dort via SMS versandt. Da der NCP Secure Enterprise Management Server meist im HF-technisch abgeschirmten Rechenzentrum installiert ist, war eine Trennung dieser beiden Komponenten notwendig. Für den Fall von Installationen mit großen Benutzerzahlen bietet NCP wahlweise auch eine HTTPS-Schnittstelle zu vordefinierten SMS-Versendedienstleistern an. Das Verfahren gilt als unkompliziert und sehr sicher.

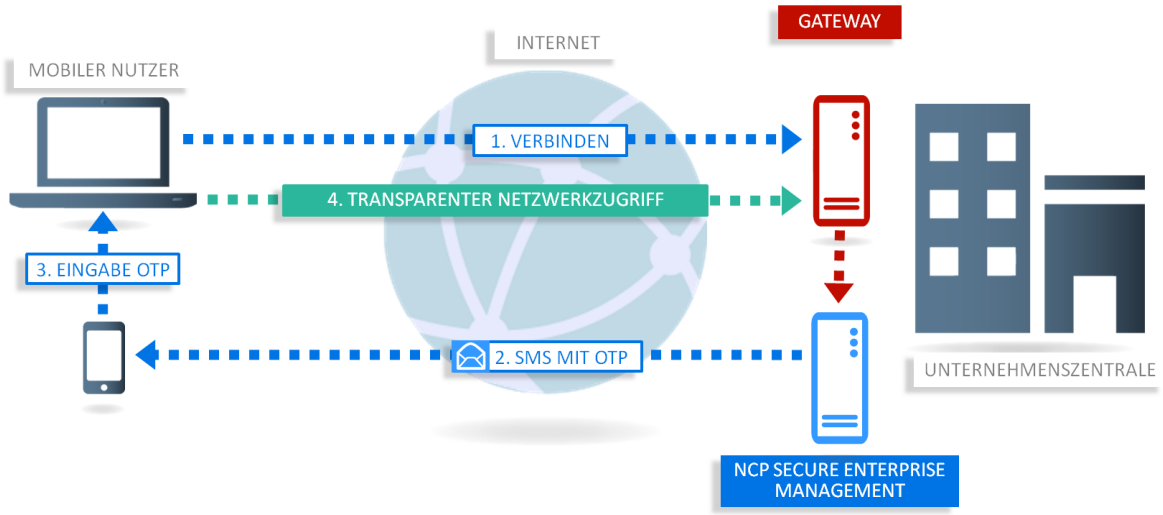


Für große und kleine Anwendungen:
Der Advanced Authentication Connector ist optimal für kleinere Installation geeignet, Installationen mit großen Benutzerzahlen nutzen eine HTTPS-Schnittstelle zu vordefinierten SMS-Versendedienstleistern.

Das NCP Secure Enterprise Management bietet alle Funktionalitäten und Automatismen, die für die Inbetriebnahme eines Remote Access-Projekts und den Dauerbetrieb in VPN-Umgebungen erforderlich sind. Durch die nahtlose Integration in das NCP Secure Enterprise Management, wird Administratoren ein großer Teil der Arbeit im Vorfeld und während des Roll-Out abgenommen. Als “Single Point of Administration” gestattet das SEM sowohl die zentrale und transparente Konfiguration als auch die Verwaltung aller VPN Client- und VPN Server-Komponenten. Das gilt für mobile Arbeitsplätze ebenso wie für lokale und entfernte VPN-Gateways oder High Availability Server. Die Software ermöglicht strukturierte Massen-Roll-Outs, Zertifikatsverteilung im Bulk Mode und Anpassungen von benutzerbezogenen Daten im laufenden Betrieb.

Automatisierte Vorgänge reduzieren den Admin-Aufwand

Über automatische Updates wird sichergestellt, dass die VPN Software sowie alle weiteren relevanten Komponenten für die Remote Access-Umgebung immer auf dem aktuellen Stand sind. Der Administrator stellt Software und Komponenten für alle entfernten Systeme zentral am Management Server als Update bereit. Dazu gehören neben der Software auch die Konfigurationsänderungen für die Zwei-Faktor-Authentisierung. Sollte es während der Übertragung zu Störungen kommen, bleiben der bereits vorhandene Softwarestand sowie die Konfiguration unberührt. Erst wenn alle vordefinierten Dateien vollständig und fehlerfrei übertragen wurden, findet das Update statt. Dabei werden alle Daten hochsicher, d.h. verschlüsselt im VPN-Tunnel übertragen.



Sicherheit für das Internetzeitalter:
Eine Zwei-Faktor-Authentisierung macht gestohlene Zugangsdaten wertlos und ist einfach nutzbar.

Große Unternehmen zeigen, wo die Reise hingeht. Je mehr Schwergewichte wie Microsoft, Twitter oder Google Zwei-Faktor-Authentisierung einsetzen, desto gebräuchlicher und selbstverständlicher wird die Technik für die Benutzer werden. Für VPN-Anwender gehören Token oder One-Time-Passwörter ohnehin schon zum Arbeitsalltag. Und mit Herstellern wie NCP, die Zwei-Faktor-Authentisierung so nahtlos in ihre Produkte integrieren, dass sie für den Administrator ohne Zusatzaufwand verwaltbar sind, gewinnen Firmen und Anwender gleichermaßen an Produktivität und Sicherheit.

Besitz macht sicher(er)

Haftungsausschluss
Die in diesem Dokument enthaltenen Informationen können ohne Vorankündigung geändert werden und stellen keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Warenzeichen
Alle genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

Stand April 2016

Next Generation Network Access Technology

www.ncp-e.com