REINERSCT

Case Study

Einfach umsetzbare Zwei-Faktor-Authentisierung für den Mittelstand!

Die Kraftanlagen Gruppe braucht für ihre Mitarbeiter sicheren Zugriff auf Microsoft 365. Mitarbeiter, die auf Montage unterwegs sind oder im Homeoffice arbeiten, nutzen die Firmenressourcen über eine Fernzugriffslösung. Hierbei setzt das Unternehmen den REINER SCT Authenticator ein, der mit einem immer nur kurzeitig gültigen Einmalpasswort (TOTP) sichere Zwei-Faktor-Authentisierung ohne Smartphone erlaubt. Die Lösung wurde dank einfacher Benutzung schnell angenommen und hilft, das Sicherheitsniveau der Firma insgesamt zu erhöhen.

Die Anmeldung am Rechner und an Diensten mit Nutzername und Passwort hat in Firmen Tradition. Sie ist aber schon längst nicht mehr zeitgemäß. Seit Jahren publizieren Sicherheitsunternehmen Listen mit den am häufigsten genutzten Passwörtern – die immer wieder gleich oder zumindest sehr ähnlich sind. Dazu kommen die großen Passwort-Leaks der vergangenen Jahre bei vielgenutzten Online-Diensten, die rasche Verlagerung der Arbeitsplätze aus dem Büro ins Homeoffice und der steigende Anteil mobiler Mitarbeiter mit Zugriff auf das Firmennetzwerk.
Damit fällt auch die vermeintliche Sicherheit durch die Anmeldung am lokalen Rechner im Firmennetzwerk weg. Dazu kommt erheblicher administrativer Aufwand mit klassischen Passwörtern, etwa weil Nutzer sie während ihres Urlaubs vergessen oder nicht rechtzeitig ändern. Auch die Aufgabe, vermeintlich sichere Passwörter durchzusetzen, ist nicht einfach. Nahezu unmöglich ist es sogar zu kontrollieren, ob Nutzer beruflich und privat dieselben Passwörter verwenden, um sie sich einfacher merken zu können – was aufgrund der Passwort-Leaks bei vielen privat genutzten Diensten ein erhebliches Sicherheitsrisiko ist.

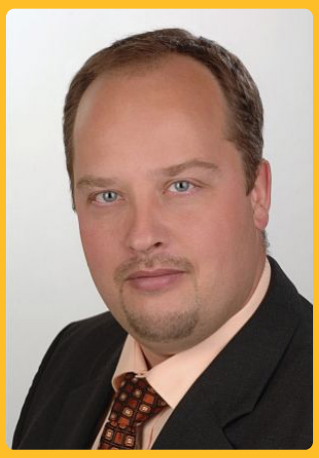
Multifaktor-Authentisierung wird Standard
Aus all diesen Gründen empfehlen Sicherheitsexperten – unter anderem das Bundesamt für Sicherheit in der Informationstechnik (BSI) – schon länger den Einsatz einer Zwei-Faktor-Authentisierung. Das BSI hat diese Empfehlung Ende Juli 2021 sogar noch einmal verschärft: Die Behörde zählt sie nun zu den Mindeststandards für die Nutzung externer Cloud-Dienste.
Ein in Firmen besonders erfolgreicher externer Cloud-Dienst ist Microsoft 365. Zwar bietet der Konzern mit dem Microsoft Authenticator dafür eine eigene Lösung an, die ist aber nicht in allen Fällen geeignet. Microsoft macht in seinem Shared Responsibility Model ganz deutlich klar, dass die Verantwortung für Benutzerkonten und -identitäten sowie die Identity- und Directory-Infrastruktur ganz oder zumindest teilweise beim Kunden liegt. Hier herrscht also dringender Handlungsbedarf.

REINER SCT Authenticator bei der Kraftanlagen Gruppe
Dies hat die Kraftanlagen Gruppe frühzeitig erkannt und setzt nun auf den REINER SCT Authenticator, eine Hardware für Zwei-Faktor-Authentifizierung mit TOTP (Time-based One-time Password/ zeitbasierendes Einmalpassword). Die Kraftanlagen Gruppe hat sich in den 1920er-Jahren als führender deutscher Anbieter im Anlagen- und Rohrleitungsbau etab-

Kraftanlagen
ENERGIES & SERVICES

Branche
Industrie, Energie und Gebäudetechnik
Produkt
REINER SCT Authenticator
Mitarbeiter
rund 2.200 Personen

Die Kraftanlagen Gruppe hat sich in den 1920er-Jahren als führender deutscher Anbieter im Anlagen- und Rohrleitungsbau etabliert und ist heute als Teil der französischen Bouygues Gruppe führender Dienstleister für Industrie, Energie und Gebäudetechnik.



Alexander Siegelin
Head of IT

”

Als wir den Authenticator vor der Einführung erst einmal ausprobiert haben, waren wir direkt von der einfachen Nutzung begeistert

liert und ist heute als Teil der französischen Bouygues Gruppe führender Dienstleister für Industrie, Energie und Gebäudetechnik. Hauptsitz der Gruppe in Deutschland ist in München. Sie beschäftigt rund 2.200 Personen, von denen etwa 1.600 regelmäßig mit Microsoft-Produkten arbeiten – immer mehr davon mit Microsoft 365 und Microsoft Teams. Etwa 600 Personen besitzen ein Firmen-Handy. In dem Fall ist das von Microsoft angebotene Verfahren mit Eingabe von Nutzername und Passwort sowie Bestätigung durch einen per SMS an das Smartphone gesandten Code möglich.

Für die etwa 1.000 weiteren Mitarbeiter musste sich Alexander Siegelin, Leiter IT bei der Kraftanlagen Gruppe, allerdings etwas anderes einfallen lassen. „Keine Multi-Faktor-Authentifizierung zu nutzen, ist heute schon fast grob fahrlässig", warnt Siegelin. „Wir wurden daher im Zuge der Umstellung unseres Microsoft-365-Mandanten auf den des Mutterunternehmens Bouygues E&S tätig."

Der erste Impuls war es – wie so oft – auch für die Authentifizierung die Microsoft-Bordmittel zu nutzen. „Allerdings wollten 50 Prozent der Teilnehmer einer Vorab-Umfrage unter unseren Beschäftigten, die kein Firmen-Handy haben, für die Authentisierung nicht ihr privates Mobiltelefon nutzen", berichtet Siegelin. Dazu sind sie auch nicht verpflichtet, schließlich müssten sie dazu mindestens ihre private Mobilfunknummer an Microsoft übermitteln.

Und nicht nur von Betriebsräten wird die Vermischung von privater und beruflicher Nutzung oft kritisch gesehen. Auch Sicherheitsaspekte sprechen dagegen – schließlich hat die Firma keine Kontrolle darüber, was Angestellte mit ihrem privaten Smartphone tun oder wo und wie sie die Anmeldung noch nutzen. Dadurch entsteht schnell eine unübersichtliche Vermengung aus privater und beruflicher Nutzung, die zusätzliche Sicherheitsrisiken birgt und sich später – etwa beim Ausscheiden eines Mitarbeiters aus der Firma – nur noch schwer entwirren lässt. Lösungen, die zur Authentisierung auf einen USB-Stick angewiesen sind, wurden geprüft aber verworfen: Teilweise soll der Zugriff, zum Beispiel auf Microsoft Teams, ausschließlich über das Smartphone erfolgen. Da sind diese Lösungen nicht praktikabel. Speziell bei der Kraftanlagen Gruppe kommt noch hinzu, dass manche Mitarbeiter bei Kunden in Bereichen arbeiten, in denen Smartphones aus Sicherheitsgründen nicht erlaubt sind, sie aber von dort für ihre Arbeit dennoch auf Firmenressourcen zugreifen müssen. Dieser Zugriff soll natürlich ebenso mit einer Zwei-Faktor-Authentisierung abgesichert werden wie auf die Microsoft-Cloud.

Praxis-Tipps für die Einführung einer Zwei-Faktor-Authentisierung

„Als wir den Authenticator vor der Einführung erst einmal ausprobiert haben, waren wir direkt von der einfachen Nutzung begeistert", erklärt Siegelin. Anwender melden sich mit dem Gerät lediglich einmal am Unternehmenskonto an. Dann schalten sie den Authenticator an, wählen das Konto aus und bestätigen mit „OK". Der angezeigte TOTP-Code ist 30 Sekunden gültig. Nach dessen Eingabe erhalten sie den gewünschten Zugriff. Alle erforderlichen Lizenzen sind beim Gerätekauf bereits enthalten, laufenden Kosten fallen nicht an.

Inzwischen hat Siegelin rund 500 Geräte bestellt. Er schätzt die kurzen Lieferzeiten und die gute Erreichbarkeit des Herstellers aus dem Schwarzwald. Damit auch Mitarbeiter, die nicht täglich am PC arbeiten, keine Berührungsängste mit dem Authenticator haben, hat Siegelin mit seinem Team ein knapp einminütiges Video produziert, in dem die Verwendung erklärt wird. Das kam bei den Mitarbeitern gut an. „Wir hatten kaum Rückfragen zur Nutzung des Produkts", berichtet Siegelin.

Die Akzeptanz erhöhte zudem, dass die Mitarbeiter den Authenticator auch privat nutzen dürfen. Er unterstützt pro Nutzer bis zu 60 Konten bei einer ständig wachsenden Liste von Services. „Ich möchte ja auch, dass die Mitarbeiter sich privat sicher verhalten", sagt Siegelin, „denn wenn privat ein Bewusstsein für IT-Sicherheit da ist, dann schalten sie das in der Arbeit nicht aus, es kommt dann also auch der Firma zugute."

Aufgrund der bisherigen guten Erfahrungen will die Kraftanlagen Gruppe den REINER SCT Authenticator auch für weitere Anwendungen nutzen. Bereits im Einsatz ist er zur Anmeldung am Social Intranet. Außerdem ist ein Single-Sign-on (SSO) über Azure Active Directory in Vorbereitung. Da ist Multi-Faktor-Authentisierung Pflicht. Damit ist schon absehbar, dass auch weitere Mitarbeiter mit dem handlichen und zuverlässigen Passwortgenerator von Reiner SCT ausgestattet werden.

REINER SCT Authenticator

- Hardware-generierte, zeitbasierte Einmal passworte (TOTP)
- hochsicher, weil ohne Internetzugang und Bluetooth-Verbindung
- kein Firmenhandy erforderlich
- günstiger und einfacher nutzbar als Hard ware-Token
- keine laufenden Kosten
- PIN schützt gegen unbefugte Benutzung
- sichert bis zu 60 Konten eines Nutzers
- Langlebigkeit (hält über 10 Jahre)
- Immer Aktuell durch Zeitsynchronisation
- Maße & Gewicht: 102 x 62,5 x 19 Millimeter, 92 Gramm.

Mehr: www.reiner-sct.com/authenticator

Über REINER SCT

REINER SCT ist anerkannter Spezialist für Sicherheit in der digitalen Welt. Das Unternehmen mit Sitz in Furtwangen im Schwarzwald entwickelt und produziert in Deutschland. Zum Portfolio gehören u.a. Lesegeräte für sicheres Online-Banking, den elektronischen Personalausweis und Bezahlterminals für Händler/Handwerker. Mit dem „Authenticator" hat REINER SCT eine Lösung für sicheren Zugriff auf Plattform-Accounts mit der Zwei-Faktor-Authentisierung geschaffen.