

TEST REINER SCT LOGIN:

Bye, bye Passwortschutz

Passwörter gelten in der IT als Sicherheitsrisiko, als Einfallstor für Phishing und andere Cyberattacken. Die Sicherheitslösung REINER SCT Login schließt die Lücke, indem sie die Windows-Anmeldung und Active Directory um eine sichere Multi-Faktor-Authentifizierung ergänzt – und so den vollständigen Verzicht auf Passwörter ermöglicht. Im Fokus stehen dabei offene OATH-Standards, eine lokale Datenhaltung sowie die Nutzung robuster Hardware-Token ... | VON BJÖRN LOENZ

TESTURTEIL SEHR GUT COMPUTERN IM HANDWERK 10-11/26

Statt Passwörter einzugeben, werden bei REINER SCT Login Codes für die Zwei-Faktor-Authentifizierung vom Smartphone oder einem Generator erstellt.

Kennwörter sind in Verruf geraten, doch in vielen Handwerksbetrieben sind sie nach wie vor die einzige Hürde beim Systemzugang. Mitarbeiter wählen dabei oft einfache Passwörter oder verwenden dieselben Zugangsdaten für verschiedene Dienste. Bei einem Datenleck stehen dann alle Tore weit offen. Der Zuwachs an mobilen Geräten und flexible Arbeitsmodelle haben das Problem zusätzlich verschärft. Mobile Endgeräte einfach zu verwalten reicht nicht mehr aus, um die Nutzeridentität verläßlich zu prüfen.

REINER SCT Login ersetzt das klassische Passwort durch eine sichere Multi-Faktor-Authentifizierung (2FA). Nutzer melden sich anstelle eines Passworts über einen sogenannten Besitzfaktor an – also über etwas, das tatsächlich vorhanden ist. Dazu gehören hardwarebasierte Einmalpasswörter, NFC-Karten oder mobile Anwendungen. Das System unterstützt gängige Open Authentication (OATH)-Standards – ein herstellerunabhängiges Authentizifizierungsverfahren – und den Challenge-Response-Algorithmus OCRA, der auf dem Frage-und-Antwort-Prinzip basiert. Administratoren können selbst festlegen, ob die Anmeldung nur ergänzt, oder das Kennwort komplett abgeschafft wird. Dank phishing-resistenter Token, beispielsweise über die betriebseigene App oder FIDO-Standards, haben unbefugte Dritte keinen Spielraum mehr, abgefangene Passwörter zu mißbrauchen. Angriffe laufen allein schon deshalb ins Leere, weil es keine mehr gibt.

Simples, vollautomatisches Verfahren

Hierfür dockt REINER SCT Login an das bestehende Microsoft Entry ID an, das als führendes System dient. Für Administratoren ist die Umgebung vertraut, da keine komplett neue Benutzerdatenbank aufgebaut werden muß. Die Installation kann man lokal im eigenen Netzwerk (On-Premise), in einer Cloud-Umgebung oder als hybrides Modell umsetzen. Für die zentrale Steuerung stellt die Software eine Management-Konsole bereit, mit der sich Dienste überwachen, Lizenzinformationen einsehen und zugewiesene Tokens verwalten lassen. Ein integriertes Servicetool auf den Windows-Clients steuert zudem die Selbstinitialisierung und entlastet die IT-Abteilung bei Diagnoseaufgaben.

Bild: Reiner SCT

Flexibel in Sachen Hardware

Bei der Hardware zeigt sich die Lösung vielseitig: Neben der REINER SCT Authenticator App für iOS und Android werden auch physische Geräte unterstützt. Dazu zählen die Hardware-TOTP-Generatoren REINER SCT Authenticator oder REINER SCT Authenticator mini, NFC-Medien wie die REINER SCT FIDO Card oder bereits vorhandene Transponder. Letztere haben den Vorteil, daß ein einziges Medium für verschiedene Szenarien wie System-Login, Zeiterfassung oder die Zutrittskontrolle zugleich verwendet werden kann.

Fazit: Mehr Sicherheit, wenig Aufwand

Windows Server und mindestens Windows 10 auf den Clients sind Voraussetzung, um REINER SCT Login einzusetzen. So werden auch solche Organisationen berücksichtigt, die nicht mit aktuellen Systemen arbeiten. Zudem empfiehlt es sich, vorab zu prüfen, welche Token-Arten eingesetzt und ob bestehende NFC-Transponder weiterverwendet werden können. Der vielleicht größte Pluspunkt des Systems ist die nahtlose Einbindung in bestehende Entry ID-Strukturen und die Flexibilität in Bezug auf die Hardware. Für die Compliance-Vorgaben mittelständischer Betriebe dürfte es zudem von Vorteil sein, daß die Technologie aus Deutschland kommt. Auf der anderen Seite erfordert REINER SCT Login eine saubere Konfiguration von Clients und Server sowie die initiale Verteilung der Tokens. Für Betriebe, die ihre Arbeitsplätze wirksam gegen Passwörter-Diebstahl absichern möchten und auf Active Directory setzen, ist das eine empfehlenswerte, praxisnahe Sicherheitslösung. <<

Reiner SCT Login	
Internet:	*https://www.reiner-sct.com*
CiH-Testurteil:	sehr gut
Preis:	auf Anfrage
Systemvoraussetzg.:	aktueller Webbrowser sowie Windows Server 2012R2, Windows 10 und höher für die Client/Server-Infrastruktur