



„Mit SMS PASSCODE können wir **schnell und einfach** einen temporären Fernzugriff auf einen externen Dienstleister einrichten, ohne ein Sicherheitsrisiko einzugehen.“

CHRISTOPH PERTL ADMINISTRATOR FÜR NETZWERK UND IT SECURITY, ÖAMTC



KUNDE
ÖAMTC



INDUSTRIE
Notfall- und Rettungsdienste



HERAUSFORDERUNG
Authentisierung bei Remote-Zugängen zur Umsetzung allgemeiner IT- Compliance-Vorgaben sowie unternehmensspezifischer Sicherheitsbestimmungen. Ablösung einer bestehenden Token-basierten Authentisierung



SYSTEME GESCHÜTZT
VPN, SSL-VPN



LÖSUNG
SMS PASSCODE Multi-Faktor-Authentifizierung (MFA)

Pannenhilfe ohne Sicherheits-pannen: ÖAMTC setzt auf SMS PASSCODE

Für die Absicherung von Remote-Zugängen zum IT-Firmennetzwerk setzt der österreichische Automobilclub ÖAMTC auf die sichere Multi-Faktor-Authentisierung mit SMS PASSCODE und löst das bisherige Hardware-Token-System ab. Mitarbeiter und Dienstleister bekommen nach korrektem Login zusätzlich ein Einmal-Passcode per Mobiltelefon zugesandt. Die Administration wird dadurch deutlich einfacher und komfortabler.

Überblick

Service, Hilfe und Rettung – der ÖAMTC. Der „Österreichische Automobil-, Motorrad- und Touring-Club“ ist ein Verein mit knapp 1,8 Millionen Mitgliedern und der größte Automobilclub Österreichs. „120“ – Die Nummer der Pannenhilfe des Clubs ist bei Mitgliedern und Nicht-Mitgliedern bestens bekannt.

Der ÖAMTC ist österreichweit an etwa 150 Standorten aktiv. Die Koordinierung der jährlich ca. 700.000 Pannen-Einsätze erfolgt über vier Zentralen. Österreichweit stehen rund 500 Einsatzfahrzeuge zur Verfügung. Als gemeinnütziger Verein erbringt der ÖAMTC aber auch andere Dienstleistungen, zum Beispiel mit der Flugrettung an derzeit 16 Standorten des Christophorus-Notarzthubschraubers.



„Die Umsetzung war in einem Tag erledigt. Spezielle Schulungen waren ebenso wenig erforderlich wie Software-Deployments auf die Mobiltelefone oder Remote-Clients.“

CHRISTOPH PERTL

ADMINISTRATOR FÜR NETZWERK UND IT SECURITY, ÖAMTC



Vernetztes Rechenzentrum

Für seine Kunden und die 3000 Mitarbeiter betreibt der ÖAMTC ein Rechenzentrum mit etwa 250 Servern, die größtenteils unter VMware virtualisiert sind. Durch den Einsatz moderner, stromsparender Technologie leistet der ÖAMTC einen Beitrag zum Umweltschutz. An den Standorten werden noch weitere 150 Server eingesetzt.

Für den gesicherten Zugriff für Home Office und Administration sind derzeit etwa 250 Remote-Zugänge beim ÖAMTC eingerichtet. Sie werden von den Mitarbeitern für die Arbeit im Home Office genutzt. Gesicherte Zugänge sind auch für administrative Tätigkeiten erforderlich, die von den ÖAMTC-Mitarbeitern, aber auch von Fremdfirmen durchgeführt werden. Dabei erfolgt die Anbindung an das Firmennetzwerk über VPN-Client oder SSL-VPN.

Dynamische Passcodes gegen Hacker und Cracker

Allgemeine Compliance-Vorgaben, aber auch interne Sicherheitsbestimmungen schreiben für die Remote-Zugänge ‚Strong Authentication‘ vor, um sensible Daten im Firmennetzwerk vor unbefugtem Zugriff zu schützen.

Die Zwei-Faktor-Authentisierung war bislang mit Hilfe einer Hardware-Token-Lösung durchgeführt worden. Das hatte zwar zuverlässig funktioniert, aber auch viele administrative Probleme mit sich gebracht, zum Beispiel bei der Verteilung und Verwaltung der Authentisierungsgeräte.

Mobiltelefon statt Hardware-Token

„Bei einer Token-Lösung ist man immer von einer bestimmten Hardware abhängig“, erklärt Christoph Pertl, Administrator für Netzwerk und IT Security beim ÖAMTC.

„Da unsere Mitarbeiter ohnehin über Firmenhandys verfügen“, so Pertl weiter, „haben wir nach einer SMS-basierten Lösung gesucht. Das System unseres bisherigen Anbieters funktionierte aber bei der Authentisierung mit dem Mobiltelefon nicht zufriedenstellend.“

Daher entschied man sich beim ÖAMTC für SMS PASSCODE. Dieses System ist direkt in den Login-Prozess integriert. Will sich ein Mitarbeiter oder Dienstleister in das Firmennetzwerk einloggen, meldet er mit einem Benutzernamen und Passwort an.



Erkennt SMS PASSCODE den korrekten Login, versendet die Software über ein eigenes GSM-Modem eine SMS mit einem Einmal-Passcode an das Handy des Anwenders. Dieser Passcode ist nur für kurze Zeit gültig und kann nur einmal verwendet werden.

Außerdem überwacht SMS PASSCODE die vom Betriebssystem generierte Session-ID während der gesamten Authentisierungsprozedur. Damit wird sichergestellt, dass sich nur der anfragende Rechner einloggen kann und sich kein Unbefugter in den Prozess einklinkt.

Schnelle und problemlose Implementierung

Mit der Einrichtung des neuen Systems wurde die SecureSolutions IT-Dienstleistung und Beratung GmbH beauftragt. Das Unternehmen installierte einen virtualisierten Authentisierungs-Server, der über das Replikationssystem des ÖAMTC auf einen Backup-Standort gesichert wird.

Schnelle und problemlose Implementierung

Mit der Einrichtung des neuen Systems wurde die SecureSolutions IT-Dienstleistung und Beratung GmbH beauftragt. Das Unternehmen installierte einen virtualisierten Authentisierungs-Server, der über das Replikationssystem des ÖAMTC auf einen Backup-Standort gesichert wird. Für den SMS-Versand wurden mehrere GSM-Modems mit Verbindung zu unterschiedlichen Mobilfunk-Providern eingesetzt, eines am Produktiv- und eines am Backup-Standort. Durch ein automatisiertes Regelwerk, basierend auf den Unternehmens-Policies, kann das neue Sicherheitssystem somit auch bei einem Ausfall der Hardware oder des Mobilfunk-Netzes nicht zum Single-Point of Failure werden.

„Die Umsetzung war in einem Tag erledigt“, freut sich der IT-Experte des ÖAMTC Christoph Pertl, „spezielle Schulungen waren ebenso wenig erforderlich wie Software-Deployments auf die Mobiltelefone oder Remote-Clients“.

SMS PASSCODE lief zunächst zwei Monate lang im Probetrieb und wird nun auch im Tagesgeschäft eingesetzt. Die Verwaltung wurde damit wesentlich vereinfacht. Soll ein Remote-Zugang gewährt werden, braucht man keinen Token mehr zu versenden. Es reicht das Einrichten eines Kontos mit der entsprechenden Mobiltelefonnummer. „Damit kann ich auch einem externen Dienstleister schnell und einfach einen temporären Remote-Zugang einrichten, ohne dabei ein Sicherheitsrisiko einzugehen“, erklärt Christoph Pertl.

Schrittweise Modernisierung

Momentan laufen die alte Token- und die moderne SMS-Authentisierung noch beide im Netzwerk. Sukzessive wird dann in nächster Zeit die gesamte Remote Access-Struktur auf SMS PASSCODE umgestellt. Für die Zukunft ist ein weiterer Ausbau auf etwa 250 Remote-Zugänge geplant.

Entrust Datacard
1187 Park Place
Shakopee, MN 55379, USA
Phone +1 952 933 1223

Entrust Datacard Denmark A/S
Park Allé 350D
2605 Brøndby, Denmark
Phone: +45 70 22 55 33

Entrust Datacard A/S
Feringasträße 6 Uderföhring,
85774 München, Deutschland
Phone: +49 89 99216407

www.entrustdatacard.com

