CASE STUDY

Entrust Datacard™
sms|passcode

„Die Einwahlprozedur für die Mitarbeiter ist, im vergleich zu früher, schneller und unkomplizierter. **Wir haben fast keine Supportfälle und damit konnten wir auch den Zeit- und Geldaufwand für den Service minimieren.**“

MARCO GIBILISCOP SENIOR SYSTEM ENGINEER BEI DER WALO BERTSCHINGER CENTRAL AG IN ZÜRICH

KUNDE
Walo Bertschinger AG

HERAUSFORDERUNG
Erhöhte Datensicherheit und kostengünstige Alternative für RSA-Token

SYSTEMUNTERSTÜTZUNG
Citrix Netscalerss

LÖSUNG
SMS PASSCODE Multi-Faktor-Authentifizierung (MFA)

Eines der größten Bauunternehmen der Schweiz sichert seine Daten mit SMS PASSCODE Multi-Faktor-Authentifizierung.

Die WALO-Gruppe ist ein traditionsreiches Familienunternehmen, das in vierter Generation geführt wird und als global tätige Firma mit breitem Tätigkeitsfeld agiert. Der Fokus liegt auf dem Bau von Oberflächen und Belägen, aber auch Hochbau, Spezialtiefbau, Betonsanierungen, Gussasphalt, Abdichtungen sowie Lärmschutz und Wasserbau zählen zum Portfolio.

Seit fast 100 Jahren setzt das Familienunternehmen Walo Bertschinger konsequent auf Qualität – bei den verwendeten Produkten und der Ausführung. Was als Betrieb für Gleis- und Straßenbau begann, bietet heute ein umfangreiches Angebot für Bauausführungen jeder Art, selbst komplexe Projekte können dank des Firmen Know-hows realisiert werden.

Neben dem Züricher Hauptsitz finden sich Niederlassungen in der ganzen Schweiz. Mittlerweile ist die WALO-Gruppe zudem international tätig. Die gelungene Verbindung von Erfahrung und Innovation macht Walo Bertschinger zum modernen, soliden Familienunternehmen. Dazu zählt auch der Informatik-Bereich.

Denn die kontinuierliche Verbesserung der Produkte sowie die internationalen Projekte werden digital erfasst und diese Daten gilt es bestmöglich zu schützen. Vor kurzem setzte das Unternehmen dafür noch RSA-Softwaretoken ein. Der

Wunsch nach Veränderung führte die IT-Verantwortlichen aber schnell zur Multi-Faktor-Authentifizierungslösung von SMS PASSCODE. Marco Gibilisco, Senior System Engineer bei der Walo Bertschinger Central AG in Zürich hatte diese Lösung bereits bei anderen Großunternehmen implementiert und war damit bestens vertraut. „Diese Lösung war ideal für unsere Ansprüche, sie verursacht keine Device-Kosten, ist leicht zu integrieren, kann hochverfügbar bereitgestellt werden, die Codezustellung ist dynamisch, der Support wird auf ein Minimum gesenkt und die Bedienung denkbar einfach“, fasst Marco Gibilisco zusammen.

Eine echte Alternative zu RSA-Softwaretoken

Für die IT-Abteilung waren die RSA-Softwaretoken nicht nur eine teure Lösung, sondern verursachten auch erheblichen Aufwand, wenn es um die Synchronisation zwischen Token und RSA-Software ging. Die RSA Server-Software ist in mehrere Komponenten aufgeteilt, die alle kompatibel zum verwendeten Token (Hardware-Device) sein müssen. Gleichzeitig war auch der Support stark gefragt, da Token ablaufen, verloren oder kaputt gehen können. Neben dem Kaufpreis verursachen Token immer wiederkehrende Kosten – von der Installierung, Registrierung, Personalisierung, Verteilung bis hin zur Systemeinbindung. Die Multi-Faktor-Authentifizierungslösung von SMS PASSCODE dagegen nutzt sowohl das geschäftliche als auch/oder das private Mitarbeiterhandy als Hardware-Token zur Code-Übermittlung. Neben der hohen Akzeptanz, der höheren Aufmerksamkeit und Wertschätzung des Mitarbeiters, ist das geschäftliche oder private Smartphone völlig supportkostenfrei. Die aufwändige Administration und Verteilung von RSA-Token bleibt der IT ebenfalls erspart.

Neben dem Thema Kostenreduktion stand das Thema Sicherheit und Zuverlässigkeit ganz oben auf der Produktagenda. Auch hier punktet die Multi-Faktor-Authentifizierungslösung von SMS PASSCODE. Die Anmeldecodes werden in Echtzeit während der Anmeldeprozedur generiert; sie werden weder gespeichert noch wieder verwendet. Dabei wird der Codeversand dynamisch an die jeweilige Anmeldesituation angepasst. Für Mitarbeiter, die sich firmenintern anmelden, ist kein Codeversand notwendig. Soll der Zugriff extern erfolgen, ist z.B. eine zusätzliche Sicherheitskomponente via persönliche PIN möglich.

Maximale Zuverlässigkeit

Standorte mit hohem Sicherheitsrisiko werden vom System identifiziert. Es erkennt, von wo sich welcher Mitarbeiter einloggt. Die Walo Bertschinger hat während der Implementierung festgelegt, welches Sicherheitsprocedere in welchen Fällen generiert werden soll – mitarbeiter- und standortbezogen. Wurde es einmal digital hinterlegt, wird es immer automatisch angewendet. Damit bietet die Multi-Faktor-Authentifizierungslösung von SMS PASSCODE maximale Sicherheit beim Remote-Zugriff über unterschiedlichste Zugänge und Remote-Access-Plattformen. Ein weiterer wichtiger Punkt für die IT-Abteilung ist die Zuverlässigkeit. Auch hier konnte die Lösung überzeugen. Die mobilfunk-zentrierte Plattform der Multi-Faktor-Authentifizierungslösung von SMS PASSCODE bietet maximale Zuverlässigkeit dank vielfältiger Zustellungsmethoden für die Code-Verschlüsselung in Echtzeit sowie einen anspruchsvollen Automatismus zur Ausfallsicherung. Ist ein SMS-Versand des Codes aus irgendeinem Grund nicht möglich, stellt die Software automatisch auf Voice-Call oder Secure E-Mail um.

Implementierung leicht gemacht

Auch die Vorteile bei der Implementierung und die hohe Nutzungsbequemlichkeit waren ausschlaggebend. Die Implementierung verlief problemlos und das, obwohl beide

Walo Bertschinger

Lösungen während der Migrationsphase von RSA zu SMS PASSCODE parallel betrieben werden mussten. Auf dem Citrix Netscaler-Hochverfügbarkeitsverbund wurde sowohl die alte RSA-Tokensoftware als auch die neue SMS PASSCODE Multi-Faktor-Authentifizierung integriert und mit Prioritäten versehen. Heute wird ausschließlich mit der neuen Authentifizierungsmethode gearbeitet. Die Multi-Faktor-Authentifizierungslösung von SMS PASSCODE wird dabei abteilungsübergreifend genutzt. Vom Fachbereich über die Bauführer, Informatiker, Personaler, Abteilungsleiter, Direktoren etc. Das Anmeldeprocedere ist klar geregelt. Die Einwahl wird durch den IT-Power User über einen festgelegten Workflow beantragt und durch den Profitzenterleiter genehmigt. Nach der Genehmigung wird die Mobile-Nummer des Nutzers im Active Directory Benutzerobjekt hinterlegt und die Mitgliedschaft in der entsprechenden Domain Global Group gewährt. Danach erfolgt die einmalige Synchronisation zwischen SMS PASSCODE Server und Active Directory Datenbank. Im Anschluss wird eine SMS versandt. Nun kann sich der externe Mitarbeiter ins Firmennetzwerk einwählen.

Fazit

„Die Einwahlprozedur für die Mitarbeiter ist, im Vergleich zu früher, schneller und unkomplizierter. Wir haben fast keine Supportfälle und damit konnten wir auch den Zeit- und Geldaufwand für den Service minimieren“, schließt Marco Gibilisco ab. Neben den positiven Auswirkungen auf Zeit und Kostenblöcke, steht die neue Multi-Faktor-Authentifizierungslösung von SMS PASSCODE auch bei den Mitarbeitern hoch im Kurs. Die Lösung via Smartphone wird immer wieder gelobt, denn die unkomplizierte, einfache Anwendung erleichtert den Alltag der Nutzer sowie der IT-Abteilung enorm.

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

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

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

www.entrustdatacard.com

Entrust Datacard™