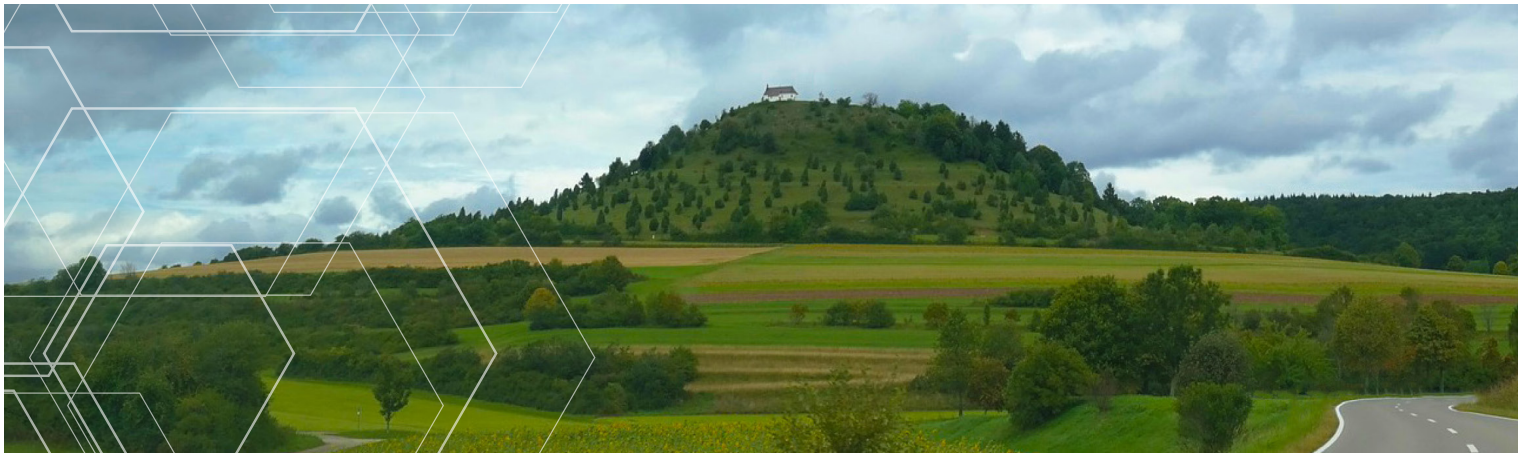
CASE STUDY



„Die Implementierung verlief überraschend einfach und schnell. **In wenigen Schritten war die neue Lösung eingebunden und einsatzbereit.**“

VOLKER KLAIBER INFORMATIONS- UND KOMMUNIKATIONSTECHNIK ZOLLERNALBKREIS

KUNDE
Zollernalbkreis

HERAUSFORDERUNG
Einfache und schnelle Remote-Verbindung in das interne Netzwerk

DIE SYSTEMUNTERSTÜTZUNG
Citrix-Anwendungen

LÖSUNG
SMS PASSCODE Multi-Faktor-Authentifizierung (MFA)

Zollernalbkreis – kommunale und staatliche Verwaltungsbehörde nutzt die SMS PASSCODE Multi-Faktor-Authentizierung

Die kommunale Behörde des baden-württembergischen Landkreises Zollernalbkreis umfasst unterschiedlichste Ämter und Dienstleistungen, vom Bau- und Jugendamt über Gesundheit, Verkehr und Verbraucherschutz.

In der Neckar-Alb-Region zwischen Stuttgart und dem Bodensee spielen Tourismus und die Wirtschaftskraft des Mittelstandes eine wichtige Rolle. Verwaltet und überwacht wird der Landkreis vom Landratsamt. Als Kreisbehörde nimmt das Landratsamt Zollernalbkreis die Aufgaben wahr, die die Leistungsfähigkeit der Gemeinden im Kreis übersteigen oder nur einheitlich erfüllt werden können. Die zusätzliche Funktion als untere staatliche Verwaltungsbehörde bringt unterschiedlichste Zusatzaufgaben mit sich: Dienstleister und Ansprechpartner für Bürgerinnen und Bürger sowie Unternehmen im Kreis, Genehmigungsbehörde, Ordnungsbehörde und Aufsichtsbehörde.

Sensible Daten zu den Einwohnern, den Unternehmen, dem Klinikum und den einzelnen Gemeinden unterliegen höchsten Sicherheitsbedürfnissen. Um diese bestmöglich zu erfüllen, nutzt der Zollernalbkreis die Multi-Faktor-Authentifizierung von SMS PASSCODE. Vor der Entscheidung für die Authentifizierungsmethode der neuesten Generation kam eine Java-basierte Authentifizierung via Hardware-Token zum Einsatz.

Das war in zweierlei Hinsicht schwierig. Zum einen verursachte die objektorientierte Programmiersprache Java bei den verwendeten ThinClients immer wieder Probleme, zum anderen kamen die typischen Nachteile externer Hardware-Token zum Tragen: verloren gegangene, vergessene oder kaputte Token, verbunden mit der Gefährdung der Datensicherheit. Zudem mussten die externen Token konfiguriert, gekauft und gewartet sowie verwaltet werden – ein zusätzlicher Kostenfaktor, trotz Outsourcing.

„Die Administration durch ein externes Rechenzentrum verstärkte die unflexible Handhabung und nahm uns ein wichtiges Kontrollelement unserer IT-Abteilung“, erklärt Volker Klaiber, Informations- und Kommunikationstechnik Zollernalbkreis. Nach intensiver Internet-Recherche fanden die IT-Spezialisten die tokenlose Multi-Faktor-Authentifizierung von SMS PASSCODE. „Die Lösung erschien uns als die beste und eingängigste für Citrix-Anwendungen. Leicht und intuitiv zu bedienen, lässt sie sich perfekt in bestehende Citrix-Umgebungen einbinden. Zudem ist es eine relativ kostengünstige Lösung“, beschreibt Volker Klaiber die Entscheidungsfindung. Auch in punkto Sicherheit lag die Multi-Faktor-Authentifizierungslösung von SMS PASSCODE ganz vorn.

„Heute verfügen wir über eine einfachere und schnellere Remoteverbindung in das interne netzwerk. Auch die akzeptanz bei den mitarbeitern ist sehr hoch.“

VOLKER KLAIBER
INFORMATIONS- UND KOMMUNIKATIONSTECHNIK ZOLLERNALBKREIS

Sichere Remote-Verbindung

Das Log-in-Verfahren mittels Einmalpasscode (OTP) bietet einen besonders hohen Schutz vor Hackerangriffen. Die Generierung des Einmalpasscodes erfolgt in Echtzeit auf einem dedizierten, meist kundeneigenen Server und ist an die jeweilige Session gebunden. Ein Trojaner kann auf dem Client zwar das Master-Kennwort erspähen, aber nicht das zweite, versendete Passcode. Es ist nicht gespeichert, weder auf dem Server noch in der Cloud.

Zudem ist das zweite Passcode nicht berechen- oder wiederverwendbar und kann nicht durch das gefürchtete »Phishing«, also das Nachahmen des Designs einer vertrauenswürdigen Anwendung wie E-Mails oder Websites, abgefragt werden. Der User-Name wird in der eigenen Datenbank geprüft, bevor er via LDAP (Anwendungsprotokoll) nochmals kontrolliert wird. Damit schützt die Multi-Faktor-Lösung auch das Hauptsystem vor DOS-Attacken.

Als weiterer Faktor bei der Authentifizierung sowie zur Anzeige des Einmalpasscodes fungiert das private Mobilfunkgerät. Der Mitarbeiter kann sein eigenes, privates Smartphone als Token verwenden und muss keine zusätzliche, risikobehaftete Hardware nur für die Netzwerknutzung mit sich tragen. Der Passcode-Transfer ist also problemlos, schnell und intuitiv abrufbar. Die Steuerung des SMS-Versandes kann vom Login-Ort abhängig gemacht werden – ganz individuell abgestimmt auf den Aufenthaltsort des Mitarbeiters, und damit schneller und auch sicherer.

Individuelle Gefährdungseinschätzung

Ändert sich der Standort eines Mitarbeiters, zum Beispiel von seiner Wohnung zum Hotel, passt der Dienst sich an die veränderten Bedingungen an – funktionell und sicherheitstechnisch. Ist beispielsweise der Handy-Empfang am neuen Standort nicht optimal, erhält der Mitarbeiter den Code per Voice-Meldung aufs Festnetz. So bietet das System verschiedene Übertragungswege um den Code bestmöglich zum Nutzer zu transportieren.

Gleichzeitig erkennt SMS PASSCODE die Gefährdungsstufe anhand des Einwahlortes, des Zeitpunktes und des verwendeten Netzwerks und wählt die erforderliche Authentifizierungsebene ganz automatisch. Diese Merkmale erkennt die Software und schätzt die Gefährdungsstufe individuell ein. So sind das Amt sowie der persönliche Wohnort ein relativ sicherer Standort, hier ist zum Teil kein Einmalpasscode nötig.

In Hotels, Beförderungsmitteln sowie bei der Nutzung öffentlicher Funknetze erhält der Mitarbeiter ohne richtiges Einmalpasscode keinen Netzwerkzugriff. Nach dem Authentifizierungsprocedere kann der Mitarbeiter dann wie gewohnt im System arbeiten. Die externen Token gehören bei den Mitarbeitern des Zollernalbkreises zur Vergangenheit und die EDV kann erhebliche Einsparungen sowie höheren Komfort für die Mitarbeiter verzeichnen. „Bei jeder Remote-Einwahl unserer Außendienstmitarbeiter, Home Office-Arbeitsplätzen etc. wird die Multi-Faktor-Authentifizierung von SMS PASSCODE von unseren Mitarbeitern genutzt“, bestätigt Volker Klaiber.

Hohe Akzeptanz bei den Mitarbeitern

„Die Implementierung verlief überraschend einfach und schnell. In wenigen Schritten war die neue Lösung eingebunden und einsatzbereit“, so Klaiber weiter. Benötigt heute ein Mitarbeiter Netzwerkzugriff – vom Firmensitz, vom Home Office oder aus dem Ausland – führt ihn die Anmeldeseite im ersten Schritt zur AD-Benutzerauthentifizierung, also zur Prüfung der Benutzeridentität auf dem persönlichen Benutzerkonto. Die gewohnte Eingabe von Name und Passwort, um sich anzumelden.

War dies erfolgreich, erscheint im nächsten Schritt ein Feld zur Eingabe des Einmalpasscodes. Eine Reihenfolge, die die Log-in-Sicherheit erhöht, denn das Echtzeit-Passcode wird erst dann generiert – einmalig und nur für diesen speziellen Log-in-Prozess. Dieses Einmalpasscode erhält der Mitarbeiter per SMS-Nachricht. Ist dieses korrekt eingegeben, erfolgt der Zugang. „Heute verfügen wir über eine einfachere und schnellere Remote-Verbindung in das interne Netzwerk. Auch die Akzeptanz bei den Mitarbeitern ist sehr hoch“, bestätigt Volker Klaiber abschließend.

Die Multi-Faktor-Authentifizierung von SMS PASSCODE ist einfach, sicher und bequem – für die IT-Abteilung ebenso wie die nutzenden Mitarbeiter. Knapp 100 Lizenzen sind in der Verwaltung des Zollernalbkreises im Einsatz, Tendenz steigend.

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