

Sichere Telearbeit mit Citrix und Utimaco

Eine Thin-Client-Lösung mit VPN- und Smartcard-Technologie sowie Single-Sign-On sorgt beim BEV für hohe Sicherheit bei bester Anwenderakzeptanz und ermöglicht das Rollout neuer Telearbeiter »Out-of-the-Box«.

Mit der Gründung der Deutschen Bahn AG wurden 1994 Funktionen und Aufgaben der ehemaligen Deutschen Bundesbahn und der ehemaligen Deutschen Reichsbahn auf das Eisenbahn-Bundesamt (EBA) sowie auf das Bundeseisenbahnvermögen (BEV) verlagert. Zu den Aufgaben des BEV gehören unter anderem die Betreuung von rund 60 000 Beamten, 228 000 Versorgungsempfängern und 5000 Tarifkräften, die Verwertung von Liegenschaften sowie amtsärztliche und sozialmedizinische Aufgaben. Um die standortunabhängige Verfügbarkeit der zentralen IT-Anwendungen sicherzustellen, wurde seitens des BEV frühzeitig eine leistungsfähige Netzinfrastruktur geschaffen, an die auch einzelne entfernte Arbeitsplätze wie Bahnärzte oder Kleinststandorte mit wenigen Mitarbeitern angebunden werden sollten.

Thin-Clients mit zahlreichen Vorteilen

Anfangs basierten diese Telearbeitsplätze auf klassischen Fat-Client-PCs. Die Mitarbeiter wählten sich dabei über ISDN in das Rechenzentrum in Bonn ein, wo die Verbindung aus Sicherheits-



gründen gekappt und der PC über eine RAS-Verbindung zurückgerufen wurde. Dieser automatische Callback hatte zur Folge, dass die Telefonleitung unabhängig vom benötigten Datenvolumen ständig belegt war. Allein die Kommunikationskosten für 30 Telearbeiter summierten sich so jährlich auf 90 000 Euro. Aber nicht nur die Kommunikationskosten bereiteten Kopfschmerzen, sondern auch die Themen Softwareverteilung und Wartung. Schnell war klar, dass dieses Vorgehen bei einem weiteren Ausbau zu kostspielig werden würde. Anfang 2003 evaluierte das BEV daher die Microsoft-Terminal-Server-/Citrix-Technologie mit Clients als Infrastrukturplattform. Im Gegensatz zu herkömmlichen Fat-Clients wird dabei die komplette Arbeitsumgebung von einem Server bereit gestellt – ein-

schließlich Betriebssystem sowie aller benötigten Applikationen und Daten.

Gemeinsam mit dem Citrix-Platinum-Partner Centracon, der einen Beratungsschwerpunkt im Bereich IT-Sicherheit hat und bereits ähnliche Projekte erfolgreich realisiert hat, konnten im Rahmen einer Voruntersuchung die elementaren technischen und ökonomischen Aspekte bestätigt werden. Damit war für das BEV der Weg frei für eine neue Architektur auf der Basis von Citrix. »Für unser Unternehmen war die Umstellung der BEV-Infrastruktur ideal, um die Leistungsfähigkeit und Skalierbarkeit der Citrix-Technologie unter Beweis zu stellen«, kommentiert Ingo Buck, Geschäftsführer der Centracon. »Es ist uns dabei gelungen, die kritischen Punkte Sicherheit, Perfor-

mance und Usability optimal zu lösen und darüber hinaus auch noch die Kosten gegenüber herkömmlichen Lösungsansätzen erheblich zu reduzieren.«

»Wissen plus Besitz« für höchste Sicherheit

Die besondere Herausforderung in dem Projekt bestand darin, die verschiedenen Sicherheitskomponenten wie VPN, Smartcard und Single-Sign-On in Einklang miteinander und mit der serverbasierten Citrix-Infrastruktur in einer NT4-Umgebung und den Thin-Clients zu bringen. Die Telearbeitsinfrastruktur wurde auf der Basis einer Windows-2000-Terminal-Server-Lösung und Citrix-Metaframe-XP realisiert. Als Arbeitsplätze wurden Thin-Client-PCs von Fujitsu Siemens mit Embedded-Windows-XP ausgewählt.

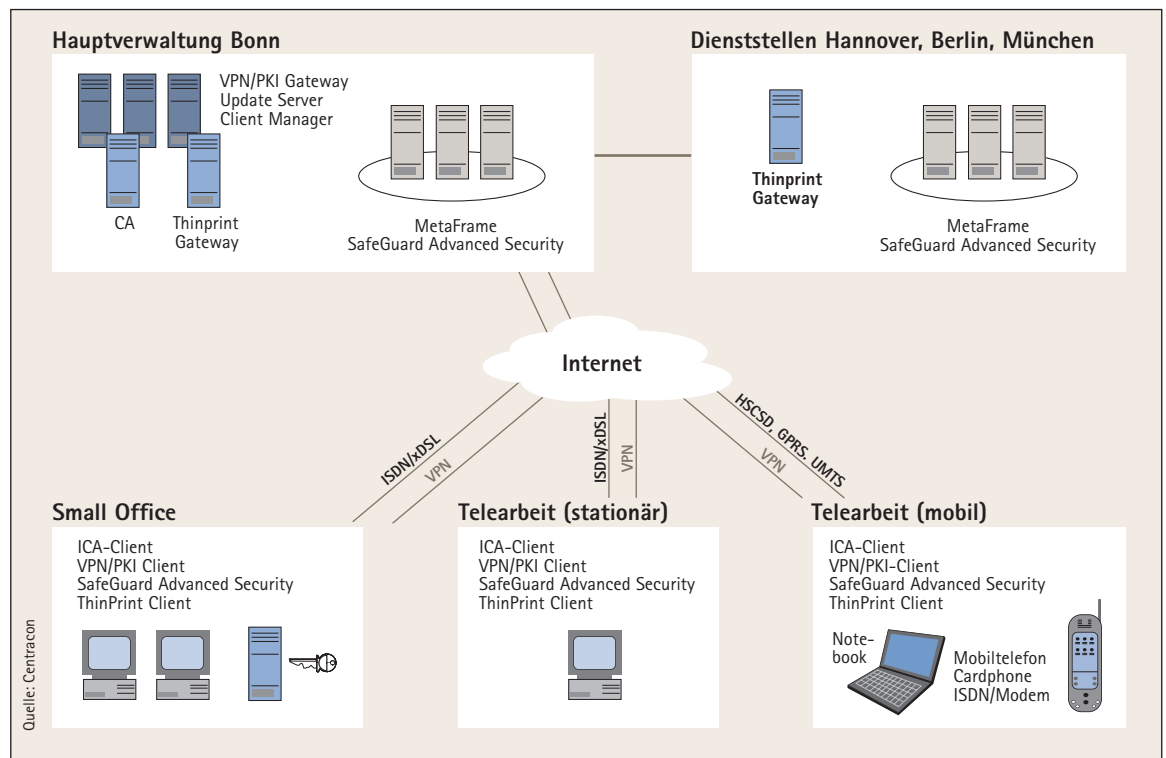
Der Einsatz der Sicherheitslösungen sollte nicht nur die Sicherheit erhöhen, sondern gleichermaßen die Benutzerfreundlichkeit steigern und eine zentrale Administration erlauben. Im Bereich der Sicherheitsinfrastruktur entschied man sich daher für die beiden deutschen Technologieanbieter NCP und Utimaco Safeware. NCP stellt dabei die auch im Rahmen des Informationsverbundes Berlin-Bonn (IVBB) eingesetzte hochsichere Remote-Access-VPN-Lösung zur Verfügung. Utimaco integriert mit ihrer modularen Sicherheitslösung »SafeGuard Advanced Security« die Smartcard-Sicherheit für Citrix und bietet die dazu notwendigen erweiterten Zugriffskontrollmechanismen. Safeguard-Advanced-Security sorgt für einen effektiven Schutz vor unerlaubtem Installieren und Ausführen von Software und ermöglicht einen schnellen und sicheren Benutzerwechsel für Arbeitsumgebungen, in denen sich mehrere Nutzer eine Arbeitsstation teilen.

Für ein durchgängig sicheres Anmeldeverfahren wird eine Lösung nach dem klassischen Sicherheitsschema »Wissen plus Besitz« auf der Basis von Smartcards genutzt. Bevor ein Anwender arbeiten kann, muss er sich mit seiner Smartcard und PIN über ein in der Tastatur des Arbeitsplatzrechners integriertes Lesegerät identifizieren. Die komfortable, einmalige Anmeldung über Single-Sign-On vereinfacht dabei das sichere Passwort-Management. Denn die eigentlichen Passwörter zur Authentisierung gegenüber dem System und den Einzelapplikationen werden nach dem Zufallsprinzip generiert und auf der Smartcard sicher geschützt gegen Auslesen gespeichert. Hier können auch längere Passwörter zum Einsatz kommen – dies erhöht nochmals die Sicherheit und den Komfort für den Benutzer, der sich nur noch eine PIN merken muss. Mittels dieser einmaligen, von Utimaco implementierten Anmeldeprozedur können sich die Anwender so gleichzeitig gegenüber dem Thin-Client, dem VPN-Tunnel, der Citrix-Umgebung sowie allen benötigten Applikationen authentisieren.

Telearbeit

»out-of-the-box«

Für ein Höchstmaß an Sicherheit läuft die gesamte Arbeitsumge-



Der Aufbau der Lösung des Bundeseisenbahnvermögens (BEV) zur Anbindung von Telearbeitsplätzen und kleineren Filialen im Überblick.

bung serverbasiert im Rechenzentrum des BEV. Bei diesem Vorgehen können Daten weder aus dem System herausgezogen noch auf die zentralen Server überspielt werden. Jegliche unberechtigte Datenhaltung und Konfiguration ist damit ausgeschlossen, sowohl in Bezug auf den Export kritischer Daten als auch auf den Import von Viren. Damit bei den künftig anstehenden Erweiterungen nicht jedes Mal komplexe Installationen notwendig sind, wurde bei der Konzeption der Lösung großer Wert auf Skalierbarkeit gelegt. Die eingesetzten Thin-Clients sind »out-of-the-box« mit einer Grundkonfiguration einsatzfähig. Bei der Erstverbindung, die ebenfalls über die Utimaco-Lösung mittels Smartcard-Anmeldung abgesichert ist, erhalten die Telearbeitsplätze remote ihre endgültige Einsatzkonfiguration inklusive Telefonbuch und allen notwendigen Lizenzen. Wächst die Anzahl der Telearbeiter oder kommen neue Dienststellen hinzu, die mittels Thin-Clients auf das Netz zugreifen wollen, ist irgendwann die Kapazitätsgrenze der Server erreicht. Bei der für das BEV realisierten Lösung lassen sich diese Kapazitäten mittels neuer Serverkomponenten im Baukastenver-

fahren erweitern. Die Installation der Terminalserver erfolgt vom Betriebssystem bis zur letzten Applikation vollständig automatisch.

Projekt trägt sich selbst

Als Sondervermögen des Bundes schaut das BEV genau auf die Kosten-Nutzen-Relation. Erste Ergebnisse kamen selbst bei vorsichtigster Kalkulation zu Projektbeginn auf etwa 15 Prozent Einsparungen in der gesamten IT-Infrastruktur, womit die technische Implementierung der Telearbeit sich von selbst bezahlt macht. Durch Umstellung auf eine VPN-Anbindung konnte die vorher genutzte RAS-Einwahl durch DSL

ersetzt werden, was bei 30 Arbeitsplätzen allein schon Einsparungen von 36 000 Euro im Jahr mit sich bringt. Mit dem neuen DSL-Tarifkonzept der Deutschen Telekom ab 01.07.2005 können pro Telearbeiter oder Small-Office künftig noch einmal 20 Euro pro Monat eingespart werden. Auch bei der Wartung der Thin-Clients werden große Beträge eingespart, da durch den kompletten Verzicht auf lokale Software nur noch Hardwareprobleme auftreten können. Ersatzgeräte können mit Kurrier- oder Paketdiensten in einem Tag vor Ort sein und konfigurieren sich bei einer Verbindung mit dem Netz selbstständig. Servicemitarbeiter, die zu einem Telearbeitsplatz fahren müssen, gehören damit der Vergangenheit an.

