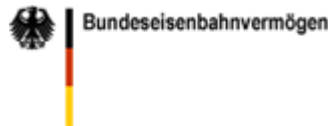


Telearbeit "Out-of-the-Box" – Mit Sicherheit ökonomisch



Ein Anwenderbericht



„Mit der neuen Telearbeitslösung sind wir erstmalig in der Lage, Telearbeiter hoch performant, zu vernünftigen Kosten und mit entsprechender Sicherheit anzubinden. Die Kombination von Citrix-, VPN- und Smartcard-Technologie ermöglicht das Rollout neuer Telearbeiter „Out-of-the-Box“, daher wollen wir sukzessive auch unsere Niederlassungen mithilfe der Citrix-Technologie anbinden.“
(Florian Doms, Referatsleiter I+K-Technik des BEV)

Die Herausforderung

Staat und Verwaltung müssen ihre Aufgaben unter den sich ständig verändernden gesellschaftlichen Bedingungen neu bestimmen. Als Dienstleister steht das BEV dabei in der Verantwortung, die Initiativen „**Bund Online 2005**“ und „**Moderner Staat**“ umzusetzen. Die Aufgaben des BEV erfordern den offensiven Einsatz moderner IT-Technik, um die standortunabhängige Verfügbarkeit der zentralen IT-Anwendungen sicherzustellen. Frühzeitig wurde daher eine leistungsfähige Netzinfrastruktur geschaffen. Schwierigkeiten bestanden jedoch bei der Anbindung einzelner entfernter Arbeitsplätze wie z.B. Bahnärzten und den Kleinststandorten mit wenigen Mitarbeitern:

Schwierigkeiten mit aktueller Lösung

- Rollout & Administration der Arbeitsplätze
- Unzureichende Sicherheitsmerkmale
- Installation von Software & Wartung vor Ort
- hohe Kosten für die Einwahlverfahren
- Geringe Leistungsfähigkeit & Flexibilität für die Telearbeiter

Im Frühjahr 2003 hatte das BEV testweise mit der Anbindung von Telearbeitern auf Basis klassischer Fat-Client-PCs begonnen. Jedoch wurden schnell Probleme der gewählten Lösung sichtbar. Die Mitarbeiter wählten sich mittels ISDN in eines der vier bundesweiten Rechenzentren ein. Von dort aus wurde die Verbindung aus Sicherheitsgründen gekappt und der PC wurde über eine RAS-Verbindung zurückgerufen. Dieses Vorgehen bedeutete jedoch, dass die Leitung, unabhängig vom notwendigen Datenvolumen, ständig offen stand. Allein die Kommunikationskosten für 30 Telearbeiter betragen so jährlich rund 90.000,- € Da bis 2005 jedoch mindestens 100 Telearbeitsplätze und später noch die Anbindung von bis zu 100 kleineren Standorten realisiert werden sollen, war schnell klar, dass dieses Vorgehen zu kostspielig werden würde.

Aber nicht nur die Kommunikationskosten bereiteten Kopfschmerzen. Je mehr Fat-Clients verteilt existieren, umso schwieriger wird das Thema Softwareverteilung. Hinzu kommt das Thema Wartung. In der Vergangenheit musste bei Problemen ein Techniker mit dem Auto zu dem jeweiligen Mitarbeiter fahren im Internet-Zeitalter ein untragbarer Anachronismus.

Das BEV war daher auf der Suche nach einer technisch passenden Lösung, die kosteneffizient und performant alle Telearbeiter anbinden kann und folgenden Anforderungen genügt:

Die Anforderungen an die Lösung

- Umsetzung „Bund Online 2005“ und „Moderner Staat“
- Ablösung durch eine an das IVBB angelehnte Sicherheitsarchitektur
- Bestmögliches Kosten-/Nutzenverhältnis
- Skalierbarkeit für die Anbindung von bis 200 Kleinststandorten
- Erhöhung der Performance für die Anwender
- Harmonisierung der Rechenzentren der 4 Hauptstandorte
- Einsparung redundanter Einwahlverfahren, Datenhaltung
- Zentrales Management aller Komponenten und der Softwareverteilung

Entscheidung zugunsten der neuen Infrastruktur

Anfang 2003 betrachtete das BEV die Microsoft Terminal Server- / Citrix-Technologie mit Thin-Clients als Infrastrukturplattform. Im Gegensatz zu herkömmlichen Fat-Clients wird die komplette Arbeitsumgebung von einem Server bereitgestellt, darunter das Betriebssystem sowie alle benötigten Applikationen und Daten. Gemeinsam mit dem externen Partner wurde eine erste Voruntersuchung durchgeführt, die auch die Aspekte der Anbindung, Sicherheit und Wirtschaftlichkeit berücksichtigen sollte. Als externen Partner fiel die Wahl auf den Citrix Platinum Partner CENTRACON, der einen parallelen Beratungsschwerpunkt im Bereich IT-Sicherheit hat und bereits ähnliche Projekte erfolgreich realisierte. Im Rahmen dieser Voruntersuchung konnten die elementaren technischen und ökonomischen Aspekte bestätigt werden, so dass sich das BEV zugunsten der neuen Architektur auf der Basis von Citrix entschied. Für die Sicherheitsinfrastruktur entschied man sich für die beiden deutschen Technologieanbieter NCP und Utimaco. NCP stellt die auch im Rahmen des Informationsverbundes Berlin-Bonn (IVBB) eingesetzte hochsichere Remote Access Lösung zu Verfügung. Utimaco integriert als Spezialanbieter Smartcard-Sicherheit für Citrix und bietet die dazu notwendige erweiterte Zugriffskontrollmechanismen.

„Citrix ist für uns eine Schlüsseltechnologie, weil wir es nicht nur für die Anbindung einzelner Telearbeiter, sondern in Zukunft auch für die Anbindung ganzer Offices und Außenstellen nutzen können“, begründet Florian Doms, Referatsleiter IT- und Kommunikationstechnik, die Entscheidung.

Im folgenden Schritt wurde in enger Zusammenarbeit mit dem BEV eine Gesamtlösung konzipiert, die sowohl die verschiedensten Sicherheitsanforderungen als auch den Ansatz der konsolidierten zentralen Bereitstellung der Arbeitsumgebung berücksichtigte:

Die Lösungskonzeption

- zentrale Bereitstellung der Arbeitsumgebung mittels Terminal Server/Citrix
- Nutzung von Thin-Clients als Telearbeitsplätze
- Integration von Smartcard-basierter Datensicherheit
- Managed VPN-Anbindung mit zentralen Update- und Verwaltungsmechanismen
- Single-Sign-On für lokale, VPN-, Citrix- und Applikations-Authentisierung
- Zentrale Userauthentisierung mittels Zertifikaten
- ausschließliche zentrale Datenablage & Internetzugang
- Zentrales optimiertes Druckmanagement mittels ThinPrint

Für die Realisierung entschied man sich für ein streng modulares Vorgehen, denn von der Projektorganisation ist das Vorgehen mehrstufig angelegt. „Wir hatten schon zu Beginn im Hinterkopf, etwas zu finden, mit dem man nicht nur einzelne Telearbeiter anbinden sondern auch mittelfristig Größeres umsetzen kann“, bestätigt Heinz Wengenroth, Referent IT-Strategie beim BEV.

Maximale Flexibilität, Sicherheit und Benutzerfreundlichkeit

Die große Herausforderung des Projektes bestand darin, die verschiedenen Sicherheitskomponenten wie VPN, Smartcard, Single-Sign-On und eine erweiterte Zugriffskontrolle in Einklang miteinander und mit der Serverbasierten Citrix-Infrastruktur und den Thin-Clients zu bringen. Der Einsatz der Sicherheitslösungen sollte nicht nur die Sicherheit erhöhen, sondern gleichermaßen die Benutzer-Freundlichkeit steigern und eine zentrale Administration erlauben. Eine nahtlose Integration der Gesamtlösung in die vorhandene IT-Struktur des BEV war in diesem Zuge obligatorisch.

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. Für die Anbindung der Telearbeitsplätze an die Hauptstelle wird die NCP SecureVPN Lösung eingesetzt, die durch LAN-Emulation am Telearbeitsplatz und die integrierte Zertifikatsbasierte Anmeldung hohe Performance mit größtmöglicher Sicherheit kombiniert. Für ein durchgängig sicheres Anmeldeverfahren eine Lösung nach dem klassischen Sicherheits-Schema „Wissen und 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. Diese Lösung von Utimaco vereint plattformübergreifend hohe Smartcard-Datensicherheit mit einem komfortablen Single-Sign-On (SSO) und erweiterter Zugriffskontrolle. Mittels dieser einmaligen Anmeldeprozedur können sich die Anwender so gleichzeitig gegenüber dem Thin-Client, dem VPN-Tunnel, der Citrix-Umgebung sowie allen benötigten Applikationen authentisieren. Für ein Höchstmaß an Sicherheit läuft zudem die gesamte Arbeitsumgebung Serverbasiert im Rechenzentrum des BEV. Bei diesem Vorgehen können Daten weder aus dem System herausgezogen noch auf die zentralen Server überspielt werden. Jegliche unberechtigte lokale Datenhaltung und Konfiguration ist damit ausgeschlossen, sowohl in Bezug auf den Export kritischer Daten als auch beim Import von Viren.

Die Implementierung dieser Gesamtlösung lief prinzipiell problemlos, die Kombination der vielen Sicherheitsanforderungen mit der zentralen Applikationsarchitektur, hat allerdings an manchen Stellen individuelle Anpassungen notwendig gemacht. Das BEV ist mit seinen umfangreichen Anforderungen in Deutschland quasi Trendsetter, und deswegen konnten bestehende Lösungen nicht ohne Weiteres 1-zu-1 übernommen werden. Gemeinsam mit dem Partner konnten diese Herausforderungen wie auch das Thema „Drucken“ optimal gelöst werden, so Alfred Dauven, Projekt- und Betriebsleiter beim BEV. Citrix Druckströme über WANs zu bewegen ist nicht trivial: Abhilfe schuf hier die deutsche ThinPrint-Lösung, mit der die Druckprozesse zentral abgearbeitet und als Streams mittels eines flexiblen Bandbreitenmanagements komprimiert zum Telearbeiter übertragen werden können. „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 GmbH. „Es ist uns dabei gelungen, die kritischen Punkte Sicherheit, Performance und Usability optimal zu lösen und darüber hinaus auch noch die Kosten gegenüber herkömmlichen Lösungsansätzen erheblich zu reduzieren.“

Telearbeit Out-of-the-Box

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. Mittels den Update- und Verwaltungsmechanismen von NCP erhalten die Telearbeitsplätze bei der Erstverbindung, die natürlich ebenfalls mittels Smartcard-Anmeldung abgesichert ist, remote ihre endgültige Einsatz-Konfiguration inkl. 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 quasi im Baukastenverfahren erweitern. Installation der Serversoftware, das Anlegen von Domänen und Einstellungen für den Zugriff auf den Data Store erfolgen vollständig automatisch.

„Zusammenfassend kann man sagen, dass wir angesichts der Komplexität des Projekts mit der Umsetzung hoch zufrieden sind“, so Heinz Wengenroth. „Mit unserer Lösung sind wir sogar zu den Richtlinien des IVBB konform und genügen auch den Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik BSI. Wir gehen davon aus, dass auch andere Behörden sich nach und nach für einen ähnlichen Weg entscheiden werden und tragen gerne zum Know-how-Transfer bei.“

Projekt finanziert 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 quasi von selbst bezahlt. Durch die Umstellung auf eine sichere VPN-Anbindung konnte die RAS-Einwahl durch DSL ersetzt werden, was bei 30 Arbeitsplätzen allein schon Einsparungen von 36.000,- € im Jahr mit sich bringt. Mit dem Ausbau der Lösung auf 100 Telearbeiter kommen weitere Einsparungen im Kommunikationsbereich von 64.000,- € hinzu. Auch bei der Wartung werden große Beträge eingespart, da durch den kompletten Verzicht auf lokale Software nur noch Hardwareprobleme auftreten können. Für einen solchen Fall wurden eine Reihe von Ersatzgeräten auf Lager gestellt, die mit Kurier- oder Paketdiensten in einem Tag vor Ort sind und dort bei einer Verbindung mit dem Netz selbständig die erforderliche Konfiguration aufspielen. Servicemitarbeiter, die zu einem Telearbeitsplatz fahren müssen, gehören damit der Vergangenheit an.

Das Projekt finanziert sich selbst

- Refinanzierung der Lösung
- Einsparungen bei den Verbindungskosten
- Reduktion der Vor-Ort-Administration / Softwareverteilung
- Günstigere Thin-Clients / längere Austauschzyklen
- Geringere Help-Desk-Kosten

„Bei dem Projekt haben uns nicht nur technische sondern auch wirtschaftliche Überlegungen getrieben – unser ROI ist damit in weniger als zwei Jahren erreicht, freut sich Florian Doms. Ein typischer PC hat heute eine maximale Lebensdauer von vier bis fünf Jahren. Bei knapp 1.300 PCs im gesamten Datenverbund des BEV müssten in Kürze bereits 360 PCs ausgetauscht werden. Durch die Erweiterung der Thin-Client-Lösung könnten diese weitere zwei Jahre verwendet werden, was einen Investitionsaufschub in Höhe von 400.000,- € darstellt. Daher arbeitet man auch mit Hochdruck an der Anbindung der Dienststellen an die Terminalserver-Umgebung. Zusätzlicher Anreiz für deren Anbindung stellt die Umstellung der veralteten X.25-Verbindungen dar, die ebenfalls durch ISDN-DSL ersetzt werden können. Zwar wird ein einziger DSL-Anschluss pro Dienststelle nicht ausreichen, dennoch existiert bei 23 Außenstellen mindestens ein jährliches Einsparpotenzial von 50.000,- €

Die Zukunft

„Wir haben gemerkt, dass man mit der Lösung viel mehr als ursprünglich geplant abdecken kann“, blickt Florian Doms zurück. „Man kann sagen, der Appetit kommt beim Essen.“ Bis Herbst 2004 sollen daher auch die kleineren Standorte, an denen bis zu vier Mitarbeiter tätig sind, mittels dieser Architektur angebunden werden. Für einen dritten Schritt wird aktuell bereits eine Machbarkeitsstudie erstellt, denn letztlich soll die Citrix Infrastruktur-Lösung auch in den großen Standorten bundesweit zum Einsatz kommen. Insgesamt geht es bei den Ausbaustufen um einen Kostenblock in Millionenhöhe, wobei schon heute eines klar ist: „Mit dem Thin-Client-Ansatz haben wir die richtige Plattform gefunden“, resümiert Florian Doms. „Performance, Sicherheit, Skalierbarkeit und vor allem die enormen Kostenvorteile sprechen eindeutig zugunsten der Terminalserver-Lösung.“

Das Bundeseisenbahnvermögen

Das Bundeseisenbahnvermögen (BEV) ist eine junge Behörde, die im Zuge der Neuordnung des Eisenbahnwesens erst 1994 entstanden ist. Mit der Gründung der Deutschen Bahn AG wurden Funktionen und Aufgaben der ehemaligen Deutschen Bundesbahn und der ehemaligen Deutschen Reichsbahn auf das Eisenbahn-Bundesamt (EBA) sowie auf das BEV verlagert. Aufgabe des BEV ist es, als moderner Dienstleister Wegbegleiter der Deutschen Bahn AG auf ihrem Weg hin zu einem leistungsstarken und zukunftsorientierten Wirtschaftsunternehmen zu sein. Zur Erfüllung dieser Aufgaben beschäftigt das BEV in seinem Kernverwaltungsbereich rund 1.000 Mitarbeiter in 10 Dienststellen und am Hauptsitz in Bonn. Zu den Aufgaben des BEV gehören unter anderem die Betreuung von rund 60.000 Beamten, 228.000 Versorgungsempfängern und 5.000 Tarifkräften, die Verwertung von Liegenschaften sowie amtsärztliche und sozialmedizinische Aufgaben.