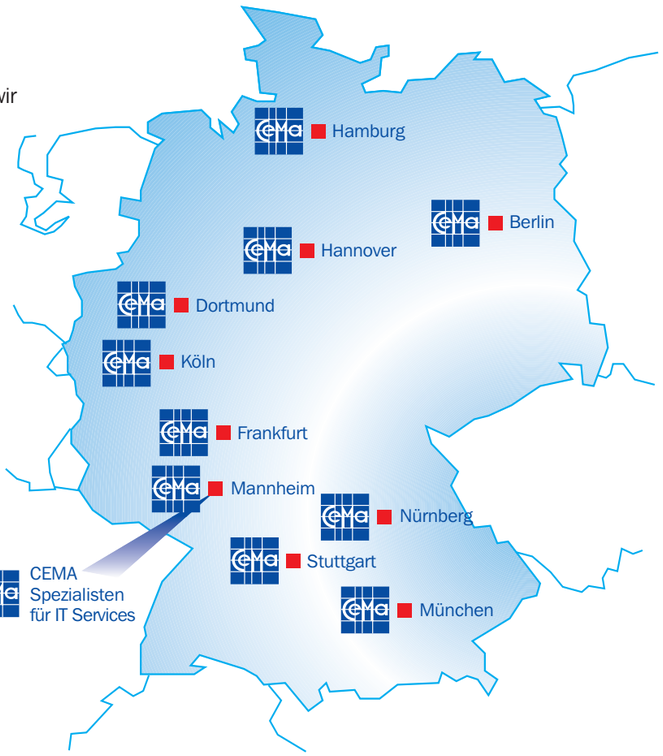
CEMA - Spezialisten für klassische IT, virtuelle IT und Cloud an neun Standorten und mit mehr als 1.440 Jahren IT-Erfahrung

Seit der Gründung 1990, quasi seit dem Beginn der PC-Netzwerk-Architektur, hat sich die CEMA auf IT-Netzwerke und -Infrastruktur spezialisiert und ist heute eines der führenden mittelständischen IT-Systemhäuser in Deutschland mit Standorten in 10 Städten und einem IT-Service Center.

Profitieren Sie von unserer Schnittstellen-kompetenz. Sie können von der Beratung bis zur Realisierung und Beschaffung alle Leistungen aus einer Hand anfordern.

Das **CEMA IT Service Center** bietet Ihnen IT-Services, Cloud- und RZ-Services, Helpdesk und 24/7 Support.

Zu unseren technischen Kernkompetenzen zählen:
Client-Management, Daten-Management, Server-Management, Security & Access, Collaboration & Mobility und IT-Infrastruktur.
Als **erfahrener Virtualisierungsspezialist** bringen wir wertvolle Projekterfahrung aus allen Bereichen mit.



Kontaktieren Sie uns.
Referenzen, Fachveranstaltungen, Stellenangebote und mehr stehen Ihnen über www.cema.de zur Verfügung **oder direkt an unseren Standorten.**

hamburg@cema.de
Tel.: (040) 30 37 432-0

berlin@cema.de
Tel.: (030) 634 128-0

hannover@cema.de
Tel.: (0511) 87 59-128

dortmund@cema.de
Tel.: (0231) 47 73 27-60

koeln@cema.de
Tel.: (0221) 78 95 63-00

helpdesk@cema.de
Tel.: (0700) 22 55 23 62

frankfurt@cema.de
Tel.: (069) 50 50 803-50

mannheim@cema.de
Tel.: (0621) 33 98-300

nuernberg@cema.de
Tel.: (0911) 689 369 - 0

stuttgart@cema.de
Tel.: (07152) 901 67-0

muenchen@cema.de
Tel.: (089) 12 59 197-10

ITSC@cema.de
Tel.: (0621) 33 98-400

www.cema.de, www.cema.de/it-blog, shop.cema.de

Hauptsitz: CEMA AG, Harrlachweg 5, 68163 Mannheim

CEMA Spezialisten für Informationstechnologie

Anwenderbericht IT-Dienstleistungszentrum Berlin (ITDZ Berlin)

ITDZ Berlin bietet der Verwaltung im Land Berlin Mobile Device Management an

Enterprise Mobility: Smart, schlank und sicher für unterschiedlichste Mobilgeräte

ITDZ BERLIN

CEMA Spezialisten für Informationstechnologie

Anwenderbericht IT-Dienstleistungszentrum Berlin (ITDZ Berlin)

ITDZ Berlin bietet der Verwaltung im Land Berlin Mobile Device Management an

iPhone, iPad und Androids am Arbeitsplatz: Bei der Verwaltung im Land Berlin ist diese Möglichkeit gegeben. Denn das IT-Dienstleistungszentrum Berlin (ITDZ Berlin) hat gemeinsam mit dem IT-Systemhaus CEMA Mobile Device Management eingeführt.
Die Lösung erfüllt nicht nur die extrem hohen Sicherheits- und Compliance-Anforderungen des Landes Berlin, sondern besticht auch durch die schlanke Integration der rund 50 Verwaltungseinheiten sowie durch die effiziente Administration der unterschiedlichsten Mobilgeräte.

Schärfste Sicherheitsvorkehrungen prägen die Informations- und Kommunikations-Infrastruktur (IKT) der Landesverwaltung Berlins
Schließlich müssen zum Teil hochsensible Daten - beispielsweise die des Senats, aber auch Personendaten der Berliner Bürger - vor unbefugtem Zugriff geschützt werden. Die mobile Kommunikation bildet da keine Ausnahme. Bislang sorgten BlackBerrys als Dienstgeräte für die erforderliche Sicherheit. Die für den Business-Einsatz konzipierten Smartphones von BlackBerry gelten als Maßstab in puncto IT-Security, doch die trendigen iPhones, iPads und Androids laufen ihnen zunehmend den Rang ab.
Für das ITDZ Berlin, das als Fullservice-Provider die entsprechende ITK Infrastruktur und Services für die rund 40.000 Nutzer im Öffentlichen Dienst Berlins bereitstellt, war klar: „Nur mit einer speziellen Softwarelösung lassen sich dienstliche Daten auf unterschiedlichen Mobilgeräten absichern, damit die Endanwender mit dem Dienstgerät ihrer Wahl arbeiten können“, erklärt Tobias Krampe, Produktmanager IT-Sicherheit und Datennetze beim ITDZ Berlin.

Umfassender Datenschutz und höchste Sicherheit
Nach einer eingehenden Marktanalyse des ITDZ Berlin fiel die Wahl auf „Dynamic Mobile Exchange“ (DME) des dänischen Herstellers Excitor. Diese Software für das Mobile Device Management erfüllt als einzige die strengen Sicherheitsvorgaben des Landes Berlin sowie das Anforderungsprofil des ITDZ Berlin.

Die geschäftlichen Daten werden auf der Betriebssystem-Ebene des Endgeräts von anderen Daten strikt isoliert. Hierzu richtet DME auf jedem Device eine spezielle verschlüsselte Unternehmenspartition ein. Aufgerufene geschäftliche Einträge (z.B. E-Mails, Kalendereinträge, Intranet Daten) werden in diesem verschlüsselten und passwortgeschützten Business-Container dargestellt und sind getrennt von den lokalen anderen Daten des Nutzers.
Im Notfall lässt sich der Business-Container über die zentrale Managementplattform vom Endgerät löschen. Bei Falscheingabe der Zugangsdaten geschieht dies automatisch.
Eine weiterer Pluspunkt der Lösung: Sämtliche Daten bleiben „inhouse”, denn die verschlüsselte und authentifizierte Kommunikation mit den Endgeräten läuft komplett über das Rechenzentrum des öffentlichen Unternehmens.

50 Verwaltungseinheiten schlank und kosteneffizient integriert
Mit der CEMA stand dem ITDZ Berlin bei der Realisierung der wichtigste deutsche Excitor-Partner zur Seite. Die CEMA ist ein erfahrener und äußerst kompetenter DME-Experte. Davon konnten wir im Projekt deutlich profitieren“, sagt Krampe.

Die geschäftlichen Daten werden auf Betriebssystem-Ebene des Endgeräts von anderen Daten strikt isoliert. Hierzu richtet DME auf jedem Device eine spezielle verschlüsselte Unternehmenspartition ein.
Aufgerufene geschäftliche Einträge (z.B. E-Mails, Kalendereinträge, Intranet Daten) werden in diesem verschlüsselten und passwortgeschützten Business-Container dargestellt und vermischen sich nicht mit den lokalen anderen Daten des Nutzers.

Die Zusammenarbeit war vorbildlich, etwa als es darum ging, die Lösung zügig einzurichten und live zu setzen, die Kommunikationsinfrastruktur anzupassen und die komplexe Verwaltungsorganisation an die Software anzubinden. Nur zwei Monate dauerte das. Das DME-Server Gateway, das für den Datentransfer zu den Endgeräten verantwortlich ist, wurde auf einer virtuellen Maschine im Netzwerk des ITDZ Berlin installiert. Die Daten erhält es von Konnektoren, die sich innerhalb des Sicherheitsnetzes des ITDZ Berlin mit dem zentralen MS Exchange Server und Active Directory synchronisieren.

Eine besondere Herausforderung beim Aufbau der DME-Hochsicherheitsarchitektur war die Anbindung der rund 50 Verwaltungseinheiten mit teilweise eigener Mailserver-Struktur und ohne Anschluss an das Active Directory der Berliner Landesverwaltung. In der Standardkonfiguration bräuchte jede Domain einen eigenen Konnektor. Nach den Vorgaben der CEMA entwickelte Excitor daher eine spezielles Add-on, mit dem sich mehrere Domains ohne spezielle Konnektoren unter einer Hauptdomain integrieren lassen. „Die schlanke Integration spart Zeit und Geld und sie erleichtert den Rollout der Lösung“, sagt Krampe.

Produktivbetrieb mit funktionalen Extras
Nach einem umfassenden internen Testbetrieb fand im Herbst 2012 die Übergabe an das Produktivsystem statt. Aktuell nutzen zehn Verwaltungen mit rund 120 Usern die Lösung. Die Zahl soll sukzessive auf 1.000 Anwender steigen, das ist bei DME flexibel und einfach gelöst. Bislang ist der Zugriff auf Kalender und E-Mails möglich. Über die DME-AppBox, die mittlerweile installiert ist, lassen sich auch Intranet-Dienste und webbasierte Anwendungen mobil nutzen.
DME mandantenfähig zu machen ist das nächste Projekt zusammen mit der CEMA. Damit erhalten die angeschlossenen Dienststellen die Möglichkeit, selbständig User zu löschen oder Geräte zu sperren.
Bereits jetzt haben sie über das lokale Active Directory volle Kontrolle darüber, welcher Mitarbeiter DME nutzen darf und welche Rechte er erhält. Dazu weisen sie über den Verzeichnisdienst einzelnen Usern oder ganzen Gruppen bestimmte Policies zu, z.B. ob etwa E-Mail-Anhänge geöffnet werden dürfen.

Tobias Krampe, Produktmanager IT-Sicherheit und Datennetze ITDZ Berlin:

„Innerhalb kurzer Zeit haben wir einen hochsicheren und zukunftsweisenden Dienst für die gesamte Berliner Landesverwaltung auf die Beine gestellt, der sowohl für die einzelnen Einrichtungen als auch für die Endanwender attraktiv ist.
Das Knowhow und die kurzen Reaktionszeiten der CEMA waren dabei wesentliche Erfolgsgaranten“, resümiert Krampe zufrieden.

ITDZ BERLIN

Auf einen Blick:

Herausforderung:
Eine Lösung einzuführen, mit der sich unterschiedlichste mobile Endgeräte effizient verwalten und gleichzeitig die extrem hohen Sicherheits- und Compliance-Anforderungen des Landes Berlin erfüllen lassen.

Nutzen:
1. Strikte Trennung zwischen geschäftlichen und anderen Daten auf dem Smart Device;
2. Erfüllung der datenschutzrechtlichen und Sicherheitsvorgaben des Landes Berlin (u.a. Daten bleiben in-house; Löschen und Sperren aus der Ferne möglich);
3. Einfache Skalierbarkeit der Lösung auf Tausende Anwender;
4. Schlanke Integration der 50 Dienststellen durch Multi-Domain-Umgebung; effiziente dezentrale Verwaltung von Usern und Geräten durch mandantenfähige Plattform;
5. Erhöhte Nutzerzufriedenheit durch freie Wahl des mobilen Dienstgeräts.

CEMA-Leistung:
Erstellen des Feinkonzepts; Installation der Lösung und Überführung in Produktivbetrieb, Konfiguration der Hochsicherheitsarchitektur; Anpassen der Kommunikationsinfrastruktur;

Systemumfeld: Microsoft Exchange Server 2003 und 2010; Active Directory; mobile Plattformen: Blackberry, iOS und Android.
Lösungstechnologie: Dynamic Mobile Exchange 4.1 von Excitor

Kunde: Das IT-Dienstleistungszentrum Berlin (www.itdz-berlin.de) ist der zentrale Dienstleister für die Berliner Verwaltung. Mit einem eigenen Landesnetz und zwei sicheren und energieeffizienten Data-Centern stellt es den Kern der IT-Infrastruktur des Landes Berlin.
Die rund 500 Mitarbeitenden unterstützen mit umfassenden Services, modernster Technik und innovativen Lösungen den reibungslosen und kosteneffizienten Betrieb der ITK-Infrastruktur und sorgen für höchste Datensicherheit.