

# Referenzbericht

## Aufbau einer modernen IT-Infrastruktur für eine soziale Einrichtung

### Der Sozialdienst katholischer Frauen e.V. Heidelberg (SkF)

ist ein Fachverband, der vor dem Hintergrund einer langen Tradition professionelle und spezialisierte Sozialarbeit anbietet.

Als kath. Fürsorgeverein für Mädchen, Frauen und Kinder 1906 ins Leben gerufen, ist er heute als Fachverband dem Caritasverband angeschlossen.

Durch die Kooperation von ehrenamtlichen und fachlich ausgebildeten hauptamtlichen Mitarbeiterinnen entsteht ein vielseitiges Angebot.

Der Fachverband kann entscheidende Unterstützung bieten in folgenden Bereichen:

Kinder- und Jugendhilfe, Beratung und Hilfe für Frauen und Familien in besonderen Not- und Konfliktsituationen, Menschen in Krisensituationen und sozial schwierigen Lebenslagen.

### Soziale Einrichtungen – hohe Anforderungen an die IT-Infrastruktur

Im Gegensatz zu einem Wirtschaftsunternehmen ist bei sozialen Einrichtungen nicht der Unternehmensgewinn das zentrale Ziel der Arbeit, sondern die Hilfe für die von der Einrichtung betreuten Menschen.

Aber auch soziale Einrichtungen müssen sich wirtschaftlichen Zwängen unterwerfen, sind sie für die Erbringung ihrer Leistungen doch häufig von öffentlichen Mitteln und Spenden abhängig.

Dies hat zur Folge, dass eine soziale Einrichtung ebenso wie ein Unternehmen auf kostensparende, leistungsfähige und effiziente Verwaltungs- und Arbeitsstrukturen angewiesen ist.

Um den effektiven Aufbau dieser Strukturen zu ermöglichen, ist auch in sozialen Einrichtungen eine moderne und leistungsstarke IT-Infrastruktur nicht mehr wegzudenken.

### Der Ist-Zustand

Bei der Analyse des Ist-Zustandes fanden wir eine dezentral organisierte IT-Infrastruktur vor. Das heißt, in jedem der 7 Standorte wurde eine unabhängige IT-Systemumgebung betrieben.

Dies hatte zur Folge, dass in jedem einzelnen Standort Hard- und Software zur Datenspeicherung und Datensicherung eingesetzt werden musste. Außerdem führte dies zu einem hohen Zeitaufwand bei der Systempflege.

So mussten z.B. für jeden einzelnen Standort Sicherheitsrichtlinien definiert, Verzeichnisstrukturen gepflegt und Softwareinstallationen an Client- und Serverumgebungen durchgeführt werden. Auch für die Datensicherung war kein einheitliches Sicherheitskonzept vorhanden.

Ein weiteres Problem bestand darin, dass die gemeinsame Datennutzung bzw. ein Datenaustausch zwischen den Standorten nur sehr umständlich zu realisieren war.

### Der Soll-Zustand

Als Fachverband, der in verschiedenen Bereichen der Kinder-, Jugend- und Familienhilfe tätig ist, verfügt der Sozialdienst katholischer Frauen e.V. Heidelberg (SkF) über eine komplexe Struktur aus Standorten, Betreuungs- und Beratungsstellen sowie verschiedenen Fachbereichen.

Um den Strukturen des SkF Heidelberg gerecht zu werden, wurden folgende Kernanforderungen für die neue IT-Infrastruktur definiert:

- ▶ Eine zentrale Datenspeicherung für alle Standorte und Fachbereiche
- ▶ Eine einheitliche Arbeitsumgebung für alle Standorte und Fachbereiche
- ▶ Ein barrierefreier, standortübergreifender Daten- und Informationsaustausch (Groupware)
- ▶ Eine wartungsarme Client-Umgebung
- ▶ Ein zentrales Sicherheitskonzept für die gesamte Organisation
- ▶ Die IT-Nutzung über Heim- und mobile Arbeitsplätze
- ▶ Die Möglichkeit, der PC- und Internetnutzung für betreute Kinder und Jugendliche (Schülernetzwerk)

Ein zentrales Ziel der Planungen bestand neben der Erhöhung der Leistungsfähigkeit und der Verbesserung des Sicherheitsstandards darin, eine Arbeitsumgebung zu schaffen, die die Mitarbeiter bei der täglichen Arbeit entlastet.

Die Bedienung der Arbeitsstationen sollte deutlich vereinfacht und mögliche Störungs- und Fehlerquellen auf ein Minimum reduziert werden.

# Referenzbericht

## Aufbau einer modernen IT-Infrastruktur für eine soziale Einrichtung

### Die Realisierung der neuen IT-Infrastruktur

Um die im Soll-Zustand definierten Leistungsmerkmale zu realisieren, wurde im ersten Schritt eine neue, zentrale Serverumgebung installiert. Zur kosteneffizienten und effektiven Hardwarenutzung wurden hierzu virtuelle Servertechnologien implementiert (mehrere virtuelle Server auf einer Hardware).

Die neue Serverumgebung realisiert die zentrale Benutzerverwaltung, die zentrale Datenspeicherung, eine zentrale Datensicherungslösung, eine Groupware- und Maillösung sowie eine einheitliche Arbeitsoberfläche für alle Mitarbeiter der 7 Standorte. Außerdem wird über sie ein separates Schülernetzwerk für Kinder und Jugendliche bereitgestellt.

Die Serverumgebung basiert auf dem aktuellen Microsoft Betriebssystem Windows Server 2008, die Arbeitsoberfläche wird den Mitarbeitern über die Windows Terminalserver Dienste bereitgestellt. Dadurch konnten die Systemanforderungen an die Clienthardware deutlich reduziert werden.

Im zweiten Schritt wurden die in der Sicherheitsrichtlinie definierten Sicherheitskomponenten installiert. Dies beinhaltet eine zentrale Firewall-Lösung, die zusätzlich zur klassischen Port-Filterung den Zugriff der Standorte auf die zentrale Serverumgebung sowie die Ferneinwahl über mobile und Heimarbeitsplätze ermöglicht (VPN-Technologie). Zusätzlich filtert die Firewall unerwünschte ein- und ausgehende Email- und Internetinhalte (Viren- und Spamschutz).

Des Weiteren wurden die Zugriffsrechte der Mitarbeiter auf Programme und Daten entsprechend der Standortzugehörigkeit und des Tätigkeitsbereiches eingeschränkt. Für die Serverumgebung wurde ein zusätzlicher Virenschutz implementiert.

Das Schülernetz wurde innerhalb eines eigenen Netzwerkes realisiert. Durch die physische und logische Trennung des Mitarbeiternetzes und des Schülernetzes kann ein unerlaubter Zugriff auf Daten des Verwaltungs- und Mitarbeiternetzes durch Kinder und Jugendliche ausgeschlossen werden.

Für das Schülernetz wurde außerdem ein Inhaltsfilter für die Internetnutzung (nur unbedenkliche Internetinhalte können aufgerufen werden) realisiert. Der Inhaltsfilter wird zentral durch die Firewall bereitgestellt und kann durch die Schüler nicht umgangen werden. Die Nutzung der schülereigenen Arbeitsstationen wurde außerdem durch spezielle Schutzsoftware zeitlich beschränkt.

Somit ist die sichere und verantwortungsvolle Nutzung digitaler Medien durch Kinder und Jugendliche gewährleistet. Und dies mit einem geringen betreuenden Aufwand.

Abschließend wurden die einzelnen Standorte an die neue zentrale Arbeitsumgebung angebunden. Hierzu wählen sich die Arbeitsstationen in den einzelnen Standorten über eine gesicherte Internetverbindung (VPN) in den Serverstandort ein. So können die Mitarbeiter auf ihre Arbeitsumgebung und auf alle Daten und Dienste zugreifen. An den einzelnen Arbeitsstationen muss durch diese Lösung keine Software mehr installiert und gepflegt werden.

### Fazit

Die neue IT-Infrastruktur stellt dem SkF Heidelberg eine zeitgemäße, zuverlässige und leistungsfähige Systemumgebung zur Verfügung.

Sie ermöglicht den Mitarbeitern den barrierefreien und standortübergreifenden Zugriff auf ihre Arbeitsumgebung. Durch die neu geschaffenen mobilen und Heimarbeitsplätze können die Arbeitszeiten der Mitarbeiter effektiver und flexibler gestaltet werden.

Die neuen Werkzeuge zum internen Daten- und Informationsaustausch ermöglichen es, dass Arbeitsabläufe einfacher und effizienter gestaltet werden.

Gleichzeitig konnte der Wartungsaufwand für Hard- und Software deutlich reduziert werden. Auch die Anschaffungs- und Wartungskosten für Server- und Clienthardware wurden deutlich reduziert.

Darüber hinaus bietet die neue Systemumgebung durch das einheitliche Sicherheitskonzept und die neuen Sicherheitskomponenten einen deutlich höheren Schutz vor unerlaubtem Datenzugriff und Datenverlust.

Die SaiNet GmbH plant und implementiert passgenaue Hard- und Softwarelösungen für Unternehmen sowie soziale- und öffentliche Einrichtungen.

Dabei profitieren unsere Kunden von der langjährigen branchenübergreifenden Erfahrung unserer Mitarbeiter in den Bereichen Server/Client-, Netzwerk- und Sicherheitslösungen.

**SaiNet GmbH**

**Mannheimer Str. 227 • 69123 Heidelberg**

Fon: (0 62 21) 7 29 79 00 • Fax: (0 62 21) 7 26 51 88  
Mail: [info@sainet.de](mailto:info@sainet.de) • <http://www.sainet.de>