I Vorwort zum IT-Konzept 2007

1. Rückblick

Mit dem IT-Konzept der Evangelischen Landeskirche in Württemberg wurde im Jahr 2005 erstmalig in einer Zusammenstellung der technische, organisatorische und rechtliche Rahmen für den Einsatz von Informationstechnologie im Bereich der Evangelischen Landeskirche in Württemberg beschrieben.

Dafür gab es interne und externe Anstöße, die auch heute noch gelten, zum Teil haben sich die Dinge in der Richtung entwickelt, wie wir im Jahr 2005 vermutet haben.

Mit der vorliegenden aktuellen Fassung haben wir der Entwicklung im IT-Bereich in den letzten beiden Jahren Rechnung getragen und präsentieren Ihnen den aktuellen Rahmen für den Einsatz von IT in der Landeskirche Württemberg.

Folgende Trends haben sich weiterentwickelt und werden auch für die Zukunft in der IT Maßstäbe setzen:

- Bisher aufwendig gepflegte lokale Lösungen werden zunehmend durch zentral angebotene Komplettlösungen ersetzt, nicht zuletzt aus Kostengründen.
- In Verbindung mit der Anwendung definierter Standards kann eine Vereinfachung erreicht werden.
- Das Thema Datensicherheit und Datenschutz stellt bezüglich der Umsetzung immer höhere Anforderungen an die IT.

Unter Beachtung dieser Rahmenbedingungen haben wir begonnen, das Serviceangebot des Referats IT für Kirchenbezirke und -gemeinden auszuweiten. Bereits jetzt werden größere Verwaltungseinheiten im Bereich der Kirchlichen Verwaltungsstellen und Kirchenpflegen zusammen mit den Arbeitsplätzen des OKR in einem Netz betreut.

Für weitere kirchliche Verwaltungen in Kirchenpflegen und Verwaltungsstellen werden wir die Integration in das Netz anbieten.

Dabei gehen wir davon aus, dass insgesamt eine Kostensenkung im IT-Bereich erreicht werden kann, wenn die vorgenannten Ziele systematisch verfolgt werden. An den gesunkenen Verrechnungspreisen in Anlage 3 sind diese Veränderungen bereits abzulesen. Gleichzeitig ergeben sich für die kirchlichen Verwaltungen qualitative Verbesserungen im täglichen Betriebsablauf, der ohne eine funktionierende EDV heutzutage nicht mehr denkbar ist. Hier spielt auch das Thema Datensicherheit eine zunehmend wichtigere Rolle. im Bereich der Informationstechnologie im OKR werden die Vorgaben zum IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnologie schrittweise umgesetzt, die Zertifizierung in der ersten Stufe ist für 2007 vorgesehen.

2. Perspektiven

- *weitergehende Unterstützung*

  Die Reaktionen auf das IT-Konzept und die Rückmeldungen, die wir in der EDV-Kommission erhalten, zeigen deutlich, dass auf allen Verwaltungsebenen innerhalb der Landeskirche der Wunsch nach einer weitergehenden Unterstützung im EDV-Bereich besteht. Unter dem Stichwort "EDV im Pfarramt" hat sich in der EDV-Kommission bereits eine Grundsatzdebatte entwickelt. Es ist aufgrund der

vorhandenen komplexen Strukturen hier nicht mit schnellen Ergebnissen für die Betroffenen zu rechnen, aber das Thema wird in der nächsten Zeit angegangen und weiter verfolgt werden.

- *elektronische Kommunikation/eGovernment*

  Der elektronische Datenaustausch zwischen den Dienststellen hat weiter zugenommen. Um diesen sicherer zu machen, wurde in einem ersten Schritt jetzt die DatenverschlüsselungsVO technisch umgesetzt. Damit ist es möglich, E-Mails, die personenbezogene Daten beinhalten, verschlüsselt zu versenden.

  Die lange angekündigte und bereits gesetzlich verankerte "digitale Signatur" lässt hingegen weiterhin in der Umsetzung auf praxistaugliche Verfahren auf sich warten. Es ist aber davon auszugehen, dass der Umgang mit der digitalen Signatur künftig zum Standard in der elektronischen Kommunikation werden wird.

- *Schriftgutverwaltung/elektronische Vorgangsbearbeitung*

  Im Oberkirchenrat wurde jetzt mit dem Projekt "ePersAkte" im Bereich der Personalverwaltung für Pfarrerinnen und Pfarrer der Einstieg in die elektronische Vorgangsbearbeitung gewagt. Schon in der Anfangsphase zeigt sich, dass die Umsetzung entscheidend von den organisatorischen Vorarbeiten (beginnend mit einer umfassenden Beschreibung der Geschäftsprozesse) abhängig ist. Konkret ist für eine elektronische Vorgangsbearbeitung zu allererst ein funktionierender aktueller Aktenplan notwendig.

- *Portale/mobiler Zugriff*

  An verschiedenen Stellen haben wir mittlerweile die Möglichkeit, über Portale auf Informationen in der Landeskirche zugreifen zu können. Von der Abdeckung des einfachen Informationsbedarfs, wie er über den Internetauftritt der Landeskirche und das Bildungsportal möglich ist, bis zum Zugriff auf konkrete Anwendungen reicht die Spanne.

  Im Bereich des neuen Kirchlichen Finanzmanagements bieten wir mit unserem CITRIX-Portal hier einen komfortablen und zugleich sicheren Zugriff auf die jeweils eigenen Daten der Dienststelle.

  Der weitere Ausbau dieses Angebots ist absehbar. Mit dieser Technik wird auch die Telearbeit weiter gefördert, da außer einem funktionierenden Internetzugang keine zusätzlichen Anforderungen vor Ort benötigt werden, die Daten liegen geschützt und gesichert hinter der Firewall der zentralen Serverumgebung.

- *Fundraising*

  Unter dieser englischen Vokabel wird gemeinhin das professionelle Einwerben von Spenden verstanden. Dafür stehen verschiedene (Standard)-Anwendungen im EDV-Bereich zur Verfügung. Wir prüfen derzeit mit dem Fundraising-Beauftragten der Landeskirche und betroffenen Dienststellen in der Landeskirche und im OKR deren Praxistauglichkeit. Es ist davon auszugehen, dass am Ende dieser Prüfung die Aufnahme einer Software in die Liste der Grundverfahren stehen wird.

3. Ziele und Rahmenbedingungen (aus dem IT-Konzept 2005)

Die Informationstechnologie der Evangelischen Landeskirche Württemberg, nachstehend IT genannt, unterstützt die Verwaltung im Oberkirchenrat und in den Dienststellen in den Kirchengemeinden und -bezirken der Landeskirche. Sie stellt im Rahmen der strategischen Leitlinien das interne und externe Angebot für eine ganzheitliche EDV Unterstützung zur Verfügung.

Ausgehend von den strategischen Zielen der IT beschreibt das vorliegende IT-Konzept die generellen Grundsätze und Voraussetzungen des IT-Angebotes. Neben diesen eher allgemeingültig formulierten Aufgaben und Standards liegt ein konkretes Leistungsangebot vor.

Gleichzeitig wird der technische, organisatorische und z. T. auch rechtliche Rahmen für den Einsatz der Informationstechnologie im Bereich der Evangelischen Landeskirche in Württemberg beschrieben.

3.1. Warum ein IT-Konzept der Evangelischen Landeskirche in Württemberg?

Bereits seit Jahren, sogar Jahrzehnten, wird die kirchliche Arbeit durch den Einsatz der Elektronischen Datenverarbeitung unterstützt und effizienter gemacht. Die Verarbeitung der kirchlichen Gemeindegliederdaten, Programme zur Unterstützung des kirchlichen Haushalts-, Kassen- und Rechnungswesens sowie zur Erstellung der Gehaltsabrechnungen kirchlicher Mitarbeiterinnen und Mitarbeiter bilden neben der Bürokommunikation und der Nutzung des Internets die Schwerpunkte.

Für eine solche Zusammenfassung gibt es interne und externe Anstöße:

- *Regelungsbedarf*

  Die immer komplexer werdenden technischen Rahmenbedingungen machen es notwendig, die tägliche Arbeit im IT-Bereich systematisch zu erfassen und zu ordnen.

  Die Definition von Standards ist ein notwendiger erster Schritt und Vorrausetzung für zukunftsfähige, wirtschaftliche und sichere Anwendung der IT.

- *Zukunftsfähigkeit*

  Um eine EDV-Landschaft systematisch weiterentwickeln zu können, ist es erforderlich, aufeinander abgestimmte Standards einzusetzen, die einen weiteren Auf- und Ausbau zulassen. Eine nicht koordinierte und ungeregelte EDV wirkt als Bremse für den technischen Fortschritt und damit in Zusammenhang stehende Arbeitserleichterungen und Prozessoptimierung. An Stellen, an denen lokale Lösungen existieren, die von Einzelpersonen erstellt und gepflegt wurden, ist eine Vertretung kaum möglich. Bei Weggang der Personen entsteht oft Unsicherheit und meist ist eine grundlegende Neuordnung durch den Nachfolger notwendig.

- *Vereinfachung*

  Standards verringern die Anzahl der Probleme, die sich sonst mit der Menge der betriebenen Systeme und Software und der in Folge daraus entstehenden Schnittstellenvielfalt exponentiell vermehren.

  Durch Nutzung von Standardwendungen kann der ansonsten oft nicht unerhebliche Zeitaufwand für Systemkoordination und Fehlersuche entfallen.

- *Kostensenkung*
  Viele verschiedene Hardware-Systeme und Softwareprogramme mit den damit verbundenen Schnittstellen erfordern zur Pflege vielfältiges EDV-Wissen und viele EDV-Fachkräfte um die Systeme am Laufen zu halten. Dies verursacht erhebliche Kosten, ebenso wie die höhere Anzahl von Schnittstellenproblemen, Fehlinvestitionen in nicht kompatible Hard- und Software sowie unzureichende Kommunikation des EDV-know-hows auf mehrere Personen. Daher ist es sinnvoll, sich auf möglichst wenige, kompatible und einheitlich verwendete Hard- und Softwarekomponenten zu beschränken.

- *Datensicherheit und Datenschutz*
  Die Einhaltung der Datensicherheits- und Datenschutzbestimmungen erfordern heute gewisse Standards (Stichwort: IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnologie) die auch wir als Kirche anwenden müssen.

- *Unterstützung bei EDV-Fragen*

Aber auch in den kirchlichen Dienststellen außerhalb des Oberkirchenrats wurde das Vorhaben, ein IT-Konzept der Evangelischen Landeskirche in Württemberg zu erstellen und zu pflegen, begrüßt. Aus Stellungnahmen der im Vorfeld beteiligten Dienststellen und Verbände kommt der eindeutige Wunsch nach einer weitergehenden Unterstützung bei EDV-Fragen. Von der Pfarrervertretung wurde die Erstellung bzw. Beschreibung von Standards in der IT ausdrücklich begrüßt und gebeten, den Geltungsbereich des Systemkonzepts auf die Pfarrämter zu erweitern. Auch die Vertreter der Kirchlichen Verwaltungsstellen haben sich konstruktiv an der Diskussion beteiligt. Dies zeigt uns deutlich, dass auch in der Fläche ein Bedarf an strategischen Vorgaben und Hilfen zur konkreten Umsetzung besteht.

3.2. Was umfasst das IT-Konzept der Evangelischen Landeskirche in Württemberg?

Neben der umfassenden Auflistung vor allem der technischen Rahmenbedingungen und Standards beim Einsatz von EDV liegen die Schwerpunkte des IT-Konzepts der Evangelischen Landeskirche in Württemberg in den folgenden Bereichen:

- Beschrieben werden die technischen Rahmenbedingungen und Standards beim Einsatz von EDV in der kirchlichen Verwaltung, z. B. für den Aufbau und Betrieb von PC-Netzen, bei der Telekommunikation, für Betriebssysteme etc.

  Beschreibung und Auflistung der Standard-Komponenten und deren Software-Versionen für die Bürokommunikation: Microsoft Exchange mit Outlook (E-Mail und öffentliche Ordner), Word, Excel über den Internet-Zugang und einen PDF-Reader sowie Softwareprodukte, die nicht alle an jedem Arbeitsplatz vorhanden sein müssen (PowerPoint, Microsoft Project, Publisher, Programme zur Datenkomprimierung, ...)

- Beschreibung und Auflistung der übrigen eingesetzten Grundverfahren (Fachsoftware, die einheitlich im gesamten Bereich der Landeskirche zum Einsatz kommt wie z. B. Navision-K, KIDICAP und Personal Office oder die Meldewesenprogramme)

- Ein weiterer Schwerpunkt liegt auf der Sicherheit in der Informationstechnologie (im Bereich der Informationstechnologie im OKR wird die schrittweise Umsetzung der Vorgaben zum IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnologie angestrebt). Zu diesem Bereich gehören auch der ständig zu aktualisierende Schutz vor Viren, Würmern, Spam-Mails u. a. und der Betrieb einer Firewall zum Schutz von unberechtigten Angriffen von außen.

In weiten Teilen beschreibt das IT-Konzept der Evangelischen Landeskirche in Württemberg dabei die bestehenden Gegebenheiten und fasst die im Einsatz befindlichen Standards (z. B. für den Datenschutz) zusammen. Aufgrund der Größe des OKR-internen Netzes und der Vielzahl der dort im Einsatz befindlichen Programme nimmt die Darstellung und Beschreibung der IT-Landschaft in diesem Bereich einen großen Raum ein.

3.3. Für wen gelten die Regelungen?

Das IT-Konzept der Evangelischen Landeskirche in Württemberg ist eine Verwaltungsvorschrift, die mit Beschluss des Kollegiums vom 28. Juni 2005 in Kraft trat und in regelmäßigen Abständen durch das Dezernat 7 überarbeitet und angepasst wird.

Die Festlegung der Standards beinhaltet i. d. R. keine Entscheidung über Beschaffung und Wartung der EDV. Diese kann sowohl dezentral oder zumindest in Teilen auch zentral erfolgen. Ausnahmen sind zentral betreute Systeme wie im Finanz- und Rechnungswesen die Programme KIFIKOS und Navision-K oder KIDICAP und Personal Office im Bereich Personalwesen.

Verpflichtend
Für den Bereich ELK i. e. S., vorläufig mit Ausnahme der Pfarrämter, sind die Bestimmungen des IT-Konzepts der Evangelischen Landeskirche in Württemberg verbindlich.

Als Empfehlung
Für die Verwaltungen der Kirchengemeinden, die Pfarrämter und die Kirchenbezirke hat das IT-Konzept der Evangelischen Landeskirche in Württemberg empfehlenden Charakter. Damit sollen die Kommunikation in der Landeskirche und die Integration in ein künftiges EDV- Netz der Landeskirche sichergestellt und Fehlinvestitionen vermieden werden.

Um den Bedürfnissen kleinerer Dienststellen zu entsprechen, wird das IT-Konzept der Evangelischen Landeskirche in Württemberg um zwei Anlagen ergänzt, welche die (IT-Konzept der Evangelischen Landeskirche in Württemberg-konforme) mögliche Ausgestaltung der Informationstechnologie vor Ort beschreiben, erforderliche Hard- und Software benennen und an Beispielen die Handhabung anschaulich machen. In diesem Bereich ist Anfang des Jahres 2006 auch die erste Fortschreibung erfolgt.

Service des Referats IT
Das Referat Informationstechnologie in der Landeskirche und im Oberkirchenrat (Ref. 7.4) versteht sich als Dienstleister und bietet den Einrichtungen der Landeskirche auf der Grundlage des IT-Konzepts der Evangelischen Landeskirche in Württemberg Einzelleistungen an, die in der Regel Bereitstellung, Wartung und Beratung beinhalten. Die Umsetzung des Systemkonzepts in diesem Bereich auf Einzelleistungen erfolgt über eine Vereinbarung zwischen den Empfängern von Leistungen und dem Referat IT. Grundlage dieser Vereinbarungen sind die schriftliche Fixierung der Einzelleistungen und deren Kosten aufgrund der Preisliste des Ref. IT (Anlage 3 des IT-Konzepts der Evangelischen Landeskirche in Württemberg).

Dadurch ist eine abgestufte und variable Betreuungsintensität in verschiedenen landeskirchlichen Einrichtungen möglich, die nach Bedarf ausgebaut oder zurückgefahren werden kann. Für bestimmte Programme, etwa im Bereich des Finanz- und Rechnungswesens oder des Personalwesens, bleibt zur Sicherung der Funktionsfähigkeit die zentrale Betreuung obligatorisch.

Eine Ausweitung des Serviceangebots auf Kirchenbezirke und Kirchengemeinden ist perspektivisch denkbar, zurzeit aber noch nicht vorgesehen.

3.4. Was sind die Alternativen?

In anderen Landeskirchen werden zum Teil zentralisiertere Lösungen mit erheblichen Finanzmitteln eingesetzt. So wird z. B. in Hannover eine flächendeckende Vernetzung angestrebt. In Baden wird ein Intranet aufgebaut – damit wurden auch dort viele Standards festgelegt.

Das IT-Konzept der Evangelischen Landeskirche in Württemberg strebt keinen Zentralismus an, möchte aber vermeiden, dass sich eine Vielfalt an EDV-Lösungen, auch Insellösungen, entwickelt, die das Miteinander und die Kommunikation untereinander auf lange Sicht erschweren und die Einführung zukunftsträchtiger Technologien unmöglich oder sehr aufwendig machen würde. Ein solcher Zustand ist auch aus finanzieller Sicht nicht erstrebenswert.

Vielmehr sollte soweit wie möglich auf gemeinsame Lösungen gesetzt werden, wie die Evangelischen Landeskirche das z. B. bei der Personalabrechnung mit KIDICAP und im Bereich Haushalts-, Kassen- und Rechnungswesen mit KIFIKOS schon seit Jahren tut und mit Navision-K in erweiterter Form fortsetzen wird.

3.5. Fortschreibung des IT-Konzepts der Evangelischen Landeskirche in Württemberg

Das IT-Konzept der Evangelischen Landeskirche in Württemberg soll jährlich fortgeschrieben werden, damit der laufenden Entwicklung in der Informations- und Kommunikationstechnologie Rechnung getragen wird.

Das IT-Konzept der Evangelischen Landeskirche in Württemberg und die künftigen Fortschreibungen werden in geeigneter Weise den übrigen Verwaltungen der Landeskirche bekannt gegeben. Die beiden Anlagen zur praktischen Umsetzung in den externen Dienststellen werden ggf. in kürzeren Abständen aktualisiert, wenn dies erforderlich wird.

Die künftigen Fortschreibungen werden in der EDV-Kommission vorgestellt und beraten.

II Rechtliche und organisatorische Vorgaben

Die für die Landeskirche gültigen gesetzlichen Regelungen bezüglich der elektronischen Datenverarbeitung, Datenschutz und Datensicherheit sind hier aufgeführt. Diese Regelungen sind grundsätzlich zu beachten. Im Internet finden Sie die gesetzlichen Regelungen unter http://elk-wue.luchterhand.de/elk-wue/lpext.dll?f=templates&fn=main-h.htm&2.0, bzw. unter http://okrweb.elk-wue.de/datenschutz.

Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG.EKD)
Vom 12. November 1993 (ABl. EKD S. 505) – geändert durch Kirchengesetz vom 7. November 2002 (ABl. EKD S. 381, ber. ABl. EKD 2003 S. 1)

Datenschutzverordnung der Evangelischen Landeskirche in Württemberg
Kirchliche Verordnung zur Durchführung und Ergänzung des Kirchengesetzes über den Datenschutz vom 14. Februar 1995 AZ 11.820 Nr. 103

Datenverschlüsselungsverordnung
vom 20. Dezember 2000 AZ 87.00 Nr. 67

Datensicherungsverordnung
vom 20. Dezember 2000 AZ 87.00 Nr. 67

Computervirenschutzverordnung
vom 20. Dezember 2000 AZ 87.00 Nr. 67

Kirchliches Gesetz über Planung kirchlicher Arbeit, Finanzmanagement und Rechnungswesen in der Evangelischen Landeskirche in Württemberg (Haushaltsordnung)
vom 27. November 2003. (Abl. 61 S. 1)

Richtlinien zum Einsatz der elektronischen Datenverarbeitung
in der Evangelischen Landeskirche in Württemberg
vom 25. März 1997 AZ 87.570 Nr. 70

Ordnung über die Arbeitsbedingungen auf Arbeitsplätzen mit Geräten der Informations- und Kommunikationstechnik (Bildschirmordnung)
Beschluss der Arbeitsrechtlichen Kommission vom 22. Juli 1999 (Abl. 58 S. 286)

Kirchliches Gesetz über die Führung von Verzeichnissen betreffend die Gemeindeglieder in der Evangelischen Landeskirche in Württemberg (Kirchenregistergesetz)
vom 8. März 1991 (Abl. 54 S. 543)

– und die dazugehörigen Ausführungsverordnungen –

Synodalbeschluss zur Einführung eines neuen kirchlichen Finanzmanagements und Rechnungswesens
Beschluss der Synode der Evangelischen Landeskirche in Württemberg vom 27. November 2002.

Arbeitsrechtliche Regelung zur Telearbeit -Dienstzimmer im Privatbereich-
Beschluss der Arbeitsrechtlichen Kommission vom 8. Dezember 2006 (Abl. 62 S. 328)

Allgemeine Regelung der Arbeitsabläufe im Oberkirchenrat (Kanzleiverfügung)
Verfügung des Vorstands vom 31. Mai 2001, geändert durch Verfügung des Vorstands vom 15. Juni 2004

III Netz- und Kommunikationsstrukturen

In diesem Abschnitt werden die technischen Vorraussetzungen für eine Vernetzung im IT-Bereich beschrieben. Dabei werden neben der 'klassischen' Technologie mit Verbindungen über physische Leitungen auch die verschiedenen Ausprägungen der neu entstandenen drahtlosen Verbindungstechniken angesprochen. Dieses Kapitel gibt weiterhin Auskunft über die zum Datentransport benötigten Protokolle, ohne die ein sinnvoller Datentransport überhaupt nicht möglich wäre. Außerdem sind die zur Nutzung des Internets notwendigen Protokolle und Dienste beschrieben. Die verwendeten Abkürzungen werden in der Anlage 4 'Abkürzungsverzeichnis' erklärt. Die Beschreibungen all der technischen Voraussetzungen beziehen sich in erster Linie auf das quantitativ und qualitativ breit angelegte Netz im Oberkirchenrat, für kleinere Netzwerke gibt Anlage 1 ausreichende Hinweise.

1. Verkabelung

Um elektronische Informationen und Rechnerleistung am Arbeitsplatz zur Verfügung zu stellen, wird die Versorgung der Arbeitsplätze mit Informationen über das LAN (Local Area Net-work) sichergestellt. Das LAN hat dabei mehrere Dienste (u. a. elektronische Post, Zugriff auf Intranet-Server und auf zentrale Verfahren) zu unterstützen. Ziel einer LAN-Planung in der Evangelischen Landeskirche in Württemberg ist, dass ein LAN anwendungsunabhängig, universell einsetzbar ist und zukünftige Anforderungen ohne größere zusätzliche finanzielle Mittel abdecken kann. Dabei sind die Faktoren Wirtschaftlichkeit und Produktneutralität bei der Planung zu berücksichtigen. Der Umzug von Dienststellen kann kostengünstiger gestaltet werden, wenn die Verkabelung weiterhin genutzt werden kann. In dieser Konzeption wird zur Investitionssicherung zudem eine Aufteilung in einen passiven und einen aktiven LAN-Teil empfohlen.

Den konzeptionellen Rahmen bestimmt die europäische Norm DIN EN 50 173 Stand Juli 2000. Sie beschreibt die strukturierte Verkabelung in Form von anwendungsunabhängigen, universell einsetzbaren Netzkonzepten.

Die Technologie im LAN-Bereich ist schnelllebig. Um einigermaßen mit der neuen Technologie Schritt zu halten, ist vorgesehen, sich künftig an der LAN-Konzeption des Landes Baden-Württemberg zu orientieren. (Siehe LAN-Konzeption der Landesverwaltung Baden-Württemberg http://www.verwaltungsreform-bw.de/servlet/PB/menu/1153853/index.html)

2. Drahtlose Verbindungen

Standard	Beschreibung/Definition	Einsatz/Begründung
Funk-LAN (Wireless LAN) (WLAN)	Funk-LANs bzw. Wireless LANs (WLANs) basieren auf dem vom IEEE definierten Standard IEEE 802.11 und bieten die Möglichkeit, mit geringem Aufwand drahtlose Netze aufzubauen oder bestehende drahtgebundene Netzwerke zu erweitern. Funk-LAN-Systeme gemäß der Erweiterung des Standards 802.11b und 802.11g haben sich mittlerweile am Markt durchgesetzt (Datenrate max. 11-54 Mbit/s, Reichweite zwischen Teilnehmer und Basisstation (Access Point) max. 30-300m). Zurzeit wird ein Standard 802.11n verabschiedet, der Funkübertragungen mit höherer Bandbreite erlaubt. Ein Funk-LAN ist ein Shared-Media-Netz, d.h. mehrere Teilnehmer teilen sich die Übertragungsrate von max. 11Mbit/s. WLANs nach 802.11a mit der Erweiterung 802.11h senden im 5 GHz-Band und erreichen eine Datenrate von max. 54 Mbit/s brutto. Es existiert ein eigenes "eingebautes" Verschlüsselungsprotokoll namens "Wired Equivalent Privacy" (WEP). Mittlerweile wurde dieses Protokoll gemäß IEEE-802.11i zum "Wi-Fi Protected Access" (WPA bzw. WPA2) weiterentwickelt, das höheren Sicherheitsanforderungen entspricht.	Einsatz: Funk-LANs können zur Einbindung mobiler Geräte (auch PDAs) in ein LAN oder für Szenarien ohne verkabelte Räume eine wirtschaftliche Variante zu drahtgebundenen LANs sein. Aufgrund der bequemen Einrichtung der Netze, der Übertragung auch über Grundstücksgrenzen hinaus und evtl. falsch (vor-) konfigurierter Geräte müssen mindestens folgende Datenschutz- und Sicherheitsmaßnahmen ergriffen werden: • Netzwerkname (SSID) unterdrücken • WPA oder WPA2 Verschlüsselung einschalten (mindestens 128 bit) • Zugangsfilter im Access Point einrichten (MAC-Adressen der Teilnehmer) Weitere Maßnahmen wie VPN einrichten oder DHCP deaktivieren werden empfohlen (Näheres siehe Informationsschrift "Sicherheit im Funk-LAN" des BSI, 2003).
Bluetooth	Bluetooth ist ein Industriestandard (IEEE 802.15.1) für ein lizenzfreies Nahbereichsfunkverfahren zur drahtlosen Sprach- und Datenkommunikation zwischen IuK-Geräten. Im Vergleich zum Funk-LAN (s. o.) hat Bluetooth eine geringere Reichweite (~10m), bietet aber geringe Hardwarekosten, niedrigen Stromverbrauch und Echtzeitfähigkeit in den Bereichen Sprachübertragung und Audio-Video-Lösungen. Bluetooth wird sich voraussichtlich in der drahtlosen Übertragung zwischen Kleinstgeräten durchsetzen und die Datenübertragung mittels Infrarotverbindungen (IrDA) ablösen.	Einsatz: Bluetooth bietet sich für die drahtlose Anbindung von Peripherie-Geräten an stationäre Geräte an. Bei der Kopplung von mobilen Geräten in nicht abhörsicheren Umgebungen sind geeignete Schutzmaßnahmen zu ergreifen (Ausreichend lange PIN, nicht benutzte Dienste abschalten, Verschlüsselung). Näheres siehe Informationsschrift "Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte" (BSI, 2003)

3. Transport-Protokolle

Standard	Beschreibung/Definition	Einsatz/Begründung
TCP/IP IPv4 Internet-Standard	TCP (Transmission Control Protocol) ist ein verbindungsorientiertes Transportprotokoll. Es unterstützt die Funktionen der Transportschicht und stellt vor der Datenübertragung eine Verbindung zwischen den Instanzen her. Das Internet Protocol operiert auf Ebene 3 des OSI-Modells (ist aber nicht zu diesem konform) und sorgt für das Routing (Wegewahl). Es arbeitet verbindungslos und paketorientiert, bietet jedoch keine gesicherte Datagramm-Übergabe. Zu den Standardanwendungen von TCP/IP zählen z. B. Telnet, FTP, E-Mail oder WWW-Anwendungen.	Einsatz: TCP/IP ist das Standard-Basisprotokoll für Ende-zu-Ende-Verbindungen im Netz des OKR und zur Kopplung mit anderen Netzen generell anzuwenden. Die Adresspläne werden beim Referat IT geführt, neue Adressen werden nur vom Referat IT vergeben. Begründung: Bestandteil der einheitlichen IT-Infrastruktur.
TCP/IP IPv6 Internet-Standard	Fundstelle: IPv6 ist eine von der IETF (Internet Engineering Task Force) erarbeitete IP-Protokollversion. Die Version 6 des IP-Protokolls umfasst insbesondere folgende Erweiterungen gegenüber IPv4: • Erweiterte Adressierungsmöglichkeit (128 Bit-Adressen) • Vereinfachung des Headerformates • Neue Möglichkeiten der Dienstgüte • Verbesserte Sicherheitsaspekte (IPsec).	Einsatz: Kurzfristig besteht kein Bedarf in der Landeskirche. Mittel- bis langfristig wird sich der Bedarf entwickeln. Deshalb sollte beim Kauf von Hard- und Software bereits heute aus Gründen der Investitionssicherheit und der Wirtschaftlichkeit die Möglichkeit eines Migrationspfads zu IPv6 gefordert werden.

Standard	Beschreibung/Definition	Einsatz/Begründung
	Die Migration von IPv4 zu IPv6 vollzieht sich vor allem in den Hosts, Routern und Switches. Da die Dauer der Übergangsphase kaum vorhersehbar ist, sollte die Interoperabilität sehr lange gegeben sein. Dazu muss jeder IPv6-fähige Host auch über einen Stack für IPv4 verfügen.	Begründung: Durch die sukzessive Ergänzung der Version IPv4 um wichtige Funktionen von IPv6 ist eine Migration zu IPv6 derzeit noch nicht erforderlich und bei Mehrkosten wirtschaftlich nicht begründbar.

4. Erweitertes Netz des OKR

Standard	Beschreibung/Definition	Einsatz/Begründung
Landeskirchlicher Standard	Unter dem "erweiterten OKR-Netz" werden die bestehenden Netzverbindungen zwischen dem OKR, dem KRZ-SWD und anderen Dienststellen verstanden. Dieses Netz wird durch Verträge über Standleitungen, ATM-DSL, Richtfunkverbindungen und andere Netzverbindungen erstellt. Basis sind Router-Router-Kopplungen und eine einheitliche IP-Struktur. Dadurch können gemeinsam und kostengünstig Ressourcen und Sicherheitstechnologien (z. B. Firewall und Virenschutz) genutzt werden.	Einsatz: Verbindung zum KRZ-SWD Andere Verbindungen (DWW, Medienhaus, Kirchliche Verwaltungsstellen, Haus Birkach, Möhringen, Kirchenpflegen)

5. Anwendungs-Protokolle in Intranets

Die Nachgenannten Protokolle setzen i. d. R. direkt auf TCP/IP auf. Es sollten immer die jeweiligen TCP-Standardports genutzt werden.

Standard	Beschreibung/Definition	Einsatz/Begründung
HTTP	Fundstelle: Die Standardisierung von HTTP obliegt dem W3C (World Wide Web Consortium). HTTP (Hyper Text Transfer Protocol) ist ein allgemeines, statusloses, objektorientiertes Protokoll zur Datenübertragung im Rahmen des World Wide Web (WWW); es dient der Adressierung der Objekte über URL (Uniform Resource Locator), wickelt die Interaktion zwischen Client und Server ab und sorgt für die Anpassung der Formate zwischen Client und Server.	Einsatz: HTTP wird im Verbund des OKR-Netzes und für die Publikation von Informationen im Internet genutzt und auf der Grundlage einer Risikoanalyse eingerichtet und dementsprechend z. B. durch Firewall-Technik gesichert. Begründung: Der Betrieb der Intranets im OKR-Netz ist dem jeweiligen Sicherheitsbedarf entsprechend zu gestalten. Dies gilt im Besonderen auch für Publikation von Informationen im Internet.
HTTPS	Fundstelle: Die Standardisierung von HTTPS obliegt dem W3C (World Wide Web Consortium). HTTPS ist eine sichere Variante von HTTP, die die Dienste von SSL V. 3 (Secure Socket Layer) bzw. TLS V1.0 (Transport Layer Security) nutzt (vgl. Nr. 9.7.2). HTTPS erweitert HTTP um Authentifizierung und Datenverschlüsselung zwischen Web-Server und Web-Browser.	Einsatz: HTTPS wird überall eingesetzt, wo ein gesichertes Kommunikationsprotokoll zwischen Web-Browser und Web-Server notwendig ist. Der Einsatz erfolgt somit bei Bedarf z. B. bei Passwortabfragen, bei der Kommunikation mit dem Portal und in einem Intranet- oder Extranet-Verbund. HTTPS kann bei Bedarf über Intranet-Grenzen (auch zu anderen Intranets) hinweg genutzt werden, ohne dass eine besondere Risikoanalyse erforderlich ist.
		Sofern US-Produkte eingesetzt werden, sind die hoch sicheren Produktversionen zu nutzen bzw. darauf zu migrieren. Begründung:

Standard	Beschreibung/Definition	Einsatz/Begründung
	nicht mehr VBScript zur Anwendung. Es können theoretisch alle .NET-Programmiersprachen eingesetzt werden. In den üblichen Dokumentationen und Beispielen wird Visual Basic .NET und C# verwendet.	
PHP	PHP ist eine Skriptsprache die von einem Interpreter ausgeführt wird, der entweder als eigenständiges Programm oder als Modul installiert wird. PHP verfügt über sehr weitgehende Funktionen und ermöglicht damit komplexe Anwendungen mit geringem Aufwand zu entwickeln. PHP ist sowohl für Windows als auch für Linux verfügbar.	Einsatz: Im OKR wird PHP für Webanwendungen eingesetzt (z. B. CMS). Begründung: Einfache Programmierung und leichte Anpassung bestehender Anwendungen

9. Portal

Mit zunehmender Verbreitung der EDV werden immer mehr Informationen digital verfügbar. Um einen Effizienz-Gewinn aus diesem Wandel zu erzielen ist es notwendig diese Informationen den Nutzern auf elektronischem Wege zur Verfügung zu stellen.

Hierfür gibt es verschiedene Möglichkeiten mit entsprechenden Vor- und Nachteilen. Da die Infrastruktur zunehmend günstiger wird, ersetzt diese in weiten Bereichen den Versand von Datenträgern. Zudem ermöglicht dies eine zentrale Datenhaltung mit weniger Redundanzproblemen und einer größeren Aktualität.

Für die Bereitstellung der Informationen wird häufig ein Portal verwendet. Dieses bietet dem Benutzer einen zentralen Zugang zu einer Vielzahl von Informationen. Dieser Zugang kann sowohl authentifiziert als auch personalisiert erfolgen. Meist wird dies mit einem auf Web-Technologien basierenden System realisiert, um möglichst vielen Systemen den Zugriff zu ermöglichen.

Die Datenbasis bilden meist viele verschiedene Systeme aus denen das Portal die Informationen für den jeweiligen Benutzer zusammenstellt. Um die Anzahl der Schnittstellen, und damit auch der Probleme zu reduzieren, empfiehlt es sich die Daten in möglichst wenigen Systemen zu konsolidieren. Diese sollten offene Schnittstellen haben, die einen Import von Daten anderer Systeme ohne allzu großen Aufwand zu ermöglichen. Vor allem für Daten die wenig oder keine Änderungen mehr erfahren werden häufig Archivierungssysteme verwendet.

Im Oberkirchenrat werden viele statische Daten erzeugt, wie zum Beispiel Rundschreiben, Amtsblätter, Formulare und andere Veröffentlichungen. Des Weiteren entstehen in den vom Oberkirchenrat betreuten Systemen Ausgabe-Daten, die elektronisch archiviert werden müssen. Um dem Nutzer diese Datenmengen einfach nutzbar zur Verfügung zu stellen, empfiehlt sich ein System, das die Daten mit Metainformationen versieht und strukturiert ablegt. Zudem ist eine gute Suchmaschine über diese Daten unerlässlich.

9.1. CITRIX-Portal

Um auch nicht webfähige Anwendungen wie zum Beispiel Navision K oder Outlook sicher und benutzerbezogen über das Internet zur Verfügung stellen zu können, wird das von der Firma Citrix stammende Web-Interface in Kombination mit dem Secure Gateway eingesetzt. Damit kann ein Nutzer native Windowsanwendungen über das Internet verwenden ohne diese bei sich installiert haben zu müssen. Vorraussetzung für die Nutzung ist eine Internetanbindung mit ausreichender Bandbreite; ein Offline-Betrieb ist zurzeit nicht möglich.

Standard	Beschreibung/Definition	Einsatz/Begründung
Citrix Secure Gateway mit Web-Interface	Dieses System der Firma Citrix ermöglicht es Terminal-Server Sitzungen über eine SSL-Verbindung Nutzern mit Internetanschluss zur Verfügung zu stellen. Zur Nutzung wird auf Client-Seite lediglich ein Webbrowser benötigt.	Einsatz: Für sämtlich Clients außerhalb des OKR die eine Internet-Anbindung haben aber keinen VPN-Router, z. B. für die flächendeckende Nutzung von Navision. Begründung: Einfachere Administration, größere Freiheit bei der Auswahl der Internetanbindung der Dienststelle

10. Standardisierung von IP-QoS

Zur Erhöhung der Ausfallsicherheit in Netzwerken, zur Integration von Diensten wie Voice over IP, Videoconference over IP etc. in Datennetze und zur Optimierung von Arbeitsgruppen innerhalb einer Netzwerkarchitektur sind nachfolgende Standards aus Gründen der Investitionssicherheit und der Wirtschaftlichkeit bei der Beschaffung von aktiven Komponenten (Switch, Router) zu berücksichtigen.

Standard	Beschreibung/Definition	Einsatz/Begründung
Einrichten von Prioritäten (Quality of Service - QoS)	Durch QoS-Funktionalitäten wird im LAN sichergestellt, dass Sprache vor Daten priorisiert zum Voice Gateway oder zu einem anderen IP-Telefon im LAN übermittelt wird. Die Priorisierung ist insbesondere für Voice over IP und Videoconference over IP erforderlich. Überdies können auch unternehmenskritische Daten gegenüber weniger kritischen priorisiert werden. Zu den Layer-3 QoS-Signalisierungswerkzeugen gehören • das Resource Reservation Protocol (RSVP) und • die IP Precedence. Das Ressource Reservation Protocol dient der Reservierung von Ressourcen in den Routern/ Switching-Komponenten in einem Netzwerk. RSVP baut zuerst einen Pfad über die Router/Switching-Komponenten auf und reserviert in den Routern/Switching-Komponenten die entsprechenden Ressourcen für die nachfolgende Übertragung, die nach Verkehrsklassen unterschieden werden kann.	Einsatz: in Router und Switching-Komponenten zur Priorisierung von Datenpaketen

11. Standards für Telekommunikation

Die herkömmlichen TK-Anlagen werden schrittweise um Voice over IP–Technologie ergänzt. Nachfolgend sind insbesondere Standards für die herkömmliche Telefonie aufgeführt.

11.1. Signalisierung

Standard	Beschreibung/Definition	Einsatz/Begründung
DSS 1 (Euro ISDN) de-facto- Standard	Fundstelle: ITU-T I.411; ETS 300 102 (European Telecommunication Standard) DSS 1 (Digital Subscriber Signaling System No.1) ist ein europäisches ISDN-Protokoll für den D-Kanal. Dieses Protokoll wird einheitlich als DSS1 bezeichnet.	Einsatz: bei digitalen TK-Anlagen der Kirchlichen Verwaltung, die insbesondere mit den Vermittlungssystemen der öffentlichen Telefon-Netzbetreiber gekoppelt sind Begründung: Zukunftssicherheit: In Europa haben sich die meisten Netzbetreiber in fast allen europäischen Staaten zu der Einführung des DSS1 verpflichtet.

11.2. Software/Schnittstellen

Standard	Beschreibung/Definition	Einsatz/Begründung
Voice over IP de-facto-Standard	Voice over IP (VoIP) bezeichnet einen digitalen Sprachdienst über IP-Netze. Die Sprache wird digitalisiert und per Hard- oder Software komprimiert übertragen (siehe auch Nr. 3.3). Der Einsatz von VoIP ist insbesondere wirtschaftlich, wenn Softphones (PC mit Audio-Karte und –Boxen und einer Telefoniesoftware) und Universal-Messaging genutzt werden. Ergonomische Geräte sind am Markt verfügbar. Kleinere Defizite dieser Technik bestehen praktisch nur noch bei speziellen Funktionen wie z. B. der Chef-/Sekretärinnen-Funktion.	Einsatz: Der Einsatz erfolgt in Pilotprojekten. Vor der Beschaffung einer neuen TK-Anlage ist zu prüfen, ob VoIP eine wirtschaftlich günstigere Lösung darstellt. Insbesondere dort, wo sich die Struktur häufig ändert, oder spezielle Funktionen benötigt werden lohnt sich der Einsatz von VoIP. Verträge über herkömmliche TK-Anlagen mit mehr als 5 Jahren Laufzeit müssen dabei besonders geprüft werden. Künftig: Die Ausweitung von VoIP in der Kirchlichen Verwaltung hängt insbesondere ab von • den Ergebnissen der Pilotprojekte • dem Fortgang der Standardisierung und Realisierung im Bereich der QoS (Quality of Services) • der Verbreitung am Markt und der daraus sich entwickelnden Wirtschaftlichkeit. Begründung: Die Wirtschaftlichkeit muss sichergestellt werden.

IV Hardware und Betriebssysteme

In diesem Abschnitt werden Hardware und Betriebssysteme beschrieben. Hardware umfasst die ganze Palette an Gerätschaften, angefangen vom eigentlichen PC mit Bildschirm und Tastatur bzw. Maus bis hin zu den Peripheriegeräten, die für einen ordnungsgemäßen, d. h. zuverlässigen und sicheren EDV-Betrieb unerlässlich sind.

Bezüglich der direkten Nutzung der einzelnen PCs wird zwischen dem persönlichen Arbeitsplatzrechner (Client), den gemeinsam genutzten Rechnern (Server) und den Netzwerkkomponenten (z. B. Router, Switche...) unterschieden.

Betriebssysteme sind Programme (Software), die notwendig sind, damit die eingesetzte Hardware mit den vorgesehenen Programmen wie z. B. eine Textverarbeitung überhaupt funktioniert. Mit Hilfe der Betriebssysteme werden die eingesetzten Komponenten koordiniert und für die verschiedenen Aufgaben zur Nutzung bereitgestellt.

Auch hier ist die Beschreibung sehr breit angelegt, um die im Bereich des Netzes innerhalb des Oberkirchenrats und der angeschlossenen Dienststellen eingesetzten Geräte und Systeme einzubeziehen. Für Einzel-PCs und kleine Netzwerke genügen die in Anlage 1 beschriebenen Komponenten.

1. Hardware-Standards

In der Kirchlichen Verwaltung soll grundsätzlich so leistungsfähige Hardware beschafft werden, dass ein produktiver Einsatz über mindestens 4 Jahre möglich ist. Allerdings kann Hardware vorher ausgetauscht werden, wenn dies nach einer Wirtschaftlichkeitsrechnung haushaltswirksame Vorteile ergibt.

Standard	Beschreibung/Definition	Einsatz/Begründung
Client		
Standard-Client Landeskirchlicher Standard	Ausstattungsmerkmale: • PC mit Intel oder Intel-kompatiblem Prozessor • Grafikkarte • Netzwerkkarte • serieller und paralleler Port • USB-Port (Universal Serial Bus) • Festplatte • Maus und Tastatur • Bildschirm entsprechend der Bildschirmarbeitsplatzverordnung • Powermanagement • CD-ROM-/DVD-Laufwerk und Diskettenlaufwerk, sofern Wirtschaftlichkeits-oder Sicherheitsgründe nicht entgegen stehen • Soundkarte etwa beim Einsatz des PC als Softphone Bei Einsatz von Windows müssen die PC der von Microsoft veröffentlichten Hardware Compatibility List (HCL) entsprechen.	Einsatz: Standard-Arbeitsplatzrechner insbesondere im Kernbereich der einheitlichen Bürokommunikation im Netz des OKR, ggf. mit Integration von Fachanwendungen. Begründung: Bestandteil der einheitlichen IT-Infrastruktur
Notebook, Handheld, Blackberry	Mobile Geräte dienen der Rationalisierung, indem insbesondere im Bürokommunikations-System Terminabstimmungen getroffen werden, Passworte sicher gespeichert, Vermerke und Besprechungsprotokolle während Telearbeit (z. B. der Reisezeit etwa im Zug) oder direkt in Besprechungen erstellt, umfangreiche Dokumente und Adressverzeichnisse elektronisch in Besprechungen und auf Dienstreisen mitgenommen und Präsentationen umweltschonend elektronisch vorgeführt	Der Einsatz mobiler Geräte ist i. d. R. wirtschaftlich. Bei der Beschaffung ist zu prüfen, ob ein Gerät für mehrere Mitarbeiter genutzt wird, ob es als Ersatz für einen stationären PC benutzt wird und wie seine Nutzungsdauer erhöht werden kann.

Standard	Beschreibung/Definition	Einsatz/Begründung
	werden können. Mobile Geräte sollen so hochwertig ausgestattet beschafft werden, dass bezogen auf den jeweiligen Anwendungsfall eine möglichst lange Nutungsdauer gewährleistet ist. Vor allem sind Hauptspeicher und Platte so hochwertig zu beschaffen, dass alle in absehbarer Zeit notwendigen Office-, Projekt- Management-, Präsentations- und Fachprogramme darauf problemlos installiert und genutzt werden können. Für Notebooks bieten Dockingstationen mit Tastatur und Monitor für das ergonomische Arbeiten am Arbeitsplatz eine besonders wirtschaftliche Alternative zu normalen Arbeitsplatz- PC. Allerdings ist es in bestimmten Anwendungsfällen nach wie vor sinnvoll, die mobilen Geräte so einzurichten, dass nur wenige Arten des Informationsaustauschs möglich sind, denn dadurch werden Integrationsprobleme vermieden und die Nutzungsdauer erhöht.	Zur Datensicherheit bei mobilen Geräten vgl. das Kapitel IX über Datenschutz und Datensicherheit.
Server		
	Ausstattungsmerkmale: • 32/64-Bit-Rechner • Server müssen bei Beschaffung durch Zusatzprozessoren oder durch stärkere Prozessoren auf mindestens die doppelte Leistung aufgerüstet werden können. • Redundante Bauteile (Netzwerkkarten, Stromversorgung, Festplatten) für höhere Verfügbarkeit • ECC-Speichermodule • RAID-Systeme für DAS • Clusterfähigkeit • Aufrüstbarkeit für SAN-Integration	Einsatz: Standard-Server insbesondere im Kernbereich der einheitlichen Bürokommunikation im Netz des OKR, ggf. mit Integration von Fachanwendungen Begründung: Bestandteil der einheitlichen IT-Infrastruktur
Speicher-Subsysteme SAN		
	Die Trennung von Server (Anwendung) und Speicherfunktion ist das tragende Konzept eines SAN (Storage Area Network). Die Speichermedien werden dabei zentralisiert an ein Netzwerk gekoppelt und sind gleichberechtigte Komponente der Gesamtstruktur. Vorteile: • hohe Performance und Verfügbarkeit • zentralisierte und konsolidierte Speicherung für heterogene Systeme • einfaches und zentrales Management • verbesserte Backup/Recovery Strategien • leistungsfähige Disaster Recovery Prozeduren Ein SAN (Storage Area Network) ist ein Hochgeschwindigkeitsnetzwerk zwischen Servern (Hosts) und Speichersubsystemen. Dabei ermöglicht ein SAN eine any-to-any Verbindung durch das gesamte Netzwerk. Die traditionellen dedizierten Verbindungen zwischen Servern und Subsystemen (DAS/Direct Attached Storage) werden eliminiert. Die Speichersubsysteme werden innerhalb eines SAN unabhängig von den Servern und damit von den eingesetzten Plattformen, das heißt ein einzelnes Speichersubsystem kann einem oder mehreren Servern zugeordnet werden. In einem SAN können sowohl Server als auch Subsysteme große Daten mengen mit großer Geschwindigkeit austauschen. Für den Datenaustausch können u. a. das Fibre-Channel (FC)- oder iSCSI-Protokoll eingesetzt werden. FC erfordert spezielle Hardwarekomponenten und ist dadurch kostenintensiver, aber allgemeinen (noch) leistungsfähiger. Für iSCSI kann hostseitig dagegen eine Standardnetzwerkkarte verwen-	Einsatz: SAN-Systeme (HBA, Platten, Switches, Bandlaufwerke) werden im OKR-Netz grundsätzlich für alle Kernbereiche der Datenspeicherung und im Clusterumfeld eingesetzt. Sowohl das FC- als auch das iSCSI-Protokoll werden verwendet. Begründung: • hohe Geschwindigkeit • Skalierbarkeit • Flexibilität • vereinfachtes Speichermanagement • Sicherheit • hohe Verfügbarkeit • Clusterunterstützung

Standard	Beschreibung/Definition	Einsatz/Begründung
	det werden. Auf der Seite der Speichersubsysteme sind hier auch kostengünstigere Komponenten als im FC-Umfeld möglich. Die Speichersubsysteme selbst verfügen über die gängigen RAID-Technologien.	
Router	Router sind stark spezialisierte Rechner deren einzige Aufgabe es ist den Datenverkehr zwischen einzelnen Computer-Netzwerken zu steuern. Im OKR werden hierfür Produkte der Firma Cisco eingesetzt.	Einsatz: Überall dort. wo Netze gekoppelt werden müssen. Z. B. die Anbindung von Dienststellen an ein Rechenzentrum per ISDN oder via Internet und VPN sein. Ebenso bei der Kopplung einzelner Netz mit Standleitungen. Begründung: Strukturieren der Netzwerke und Eingrenzen des Datenverkehrs auf die betroffenen Netzwerke.
Switches und Hubs	Switches und Hubs stellen die Verbindung zwischen Rechnern und anderen Netzwerkgeräten her. Durch Schalten von gezielten dynamischen Verbindungen zwischen angeschlossenen Geräten erzielen Switches wesentlich höhere Durchsatzraten im Vergleich zu Hubs. Da Switches nur unwesentlich teurer sind, haben diese Hubs vom Markt verdrängt. Bei Switches unterscheidet man zwischen 'managed Switches' und 'unmanaged Switches'.	Einsatz: Überall dort wo mehr als zwei Netzwerkgeräte/ Rechner miteinander verbunden werden sollen. 'Managed Switches' werden vor allem in größeren Netzwerken eingesetzt, um die Verwaltung der Netzwerke zu vereinfachen und ihre Sicherheit zu erhöhen.
Firewall	Aufgabe einer Firewall ist es Computernetzwerke zu schützen. Sie filtern den Datenverkehr und beschränken diesen auf das für die Funktionalität Notwendige.	Einsatz: Überall dort wo Netze miteinander gekoppelt sind und der Datenverkehr geregelt werden muss; z. B. Internetanbindung von Computernetzwerken Begründung: Firewalls schützen die hinter ihnen liegenden Netzwerke vor nicht gewollten Zugriffen Unbefugter.
Monitore		
Ergonomische Anforderungen	Anforderung an Bildschirmgeräte: • Die Zeichen müssen scharf, deutlich und ausreichend groß sein sowie einen angemessenen Zeichen- und Zeilenabstand haben. • Das dargestellte Bild muss stabil und frei von Flimmern sein; es darf keine Verzerrungen aufweisen. • Die Helligkeit der Bildschirmanzeige und der Kontrast zwischen Zeichen und Zeichenuntergrund auf dem Bildschirm müssen einfach einstellbar sein und den Verhältnissen der Arbeitsumgebung angepasst werden können. • Der Bildschirm muss frei sein von störenden Reflexionen und Blendungen. • Das Bildschirmgerät muss frei und leicht drehbar und neigbar sein.	Einsatz von 17-Zoll-Monitoren bei Arbeiten vorwiegend unter Windows oder einer anderen grafischen Benutzeroberfläche sowie bei Navision-K-Anwendern Für CAD-, Layout- und Grafikarbeitsplätze sind mindestens 20- Zoll-Bildschirme zu empfehlen. Begründung: Ordnung über die Arbeitsbedingungen auf Arbeitsplätzen mit Geräten der Informations- und Kommunikationstechnik (Bildschirmordnung vom 22.07.1999)
TCO de-facto-Standard	Fundstelle: TCO (Tjänstemännens Central-Organisation) berücksichtigt die Anforderungen der MPR II-Norm. Das Label stellt eine Empfehlung hinsichtlich Ergonomie, Energieverbrauch, Emission und Ökologie von Monitoren, PC und Tastaturen dar. Nach TCO 92, TCO 95 und TCO 99 wurden mit dem TCO 2003 die Standards für die technischen Geräte noch weiter angehoben: • Alle TCOs verlangen jeweils Verbesserungen hinsichtlich der Sehergonomie. Bei verschiedenen Sitzhaltungen soll ein	Einsatz: Berücksichtigung des Standards beim Kauf neuer Monitore Begründung: Neue Bildschirme müssen zumindest den Standard TCO '99 erfüllen.

Standard	Beschreibung/Definition	Einsatz/Begründung
Standardisierter Firewall Internet-Standard	Die Aufgabe von Firewalls ist es, einen möglichst ungestörten Zugriff der Intranets der Ressorts auf das öffentliche Netzwerk zu gewährleisten, andererseits den unberechtigten Zugriff auf das eigene Netz zu verhindern. Ein Firewall stellt daher den einzigen Zugang des eigenen Netzes zum öffentlichen Netzwerk dar. Die Firewall beim OKR besteht in der Regel aus Hard- und Software-Komponenten, die entsprechend der Anforderung des IT-Konzepts ganz bestimmte Dienste freigeben. Durch die Konzentration des Zugangs auf eine einzelne Komponente werden das Sicherheits-Management und die Überwachungs- und Kontrollfunktionen wesentlich vereinfacht. Bei den Zugriffskontrollsystemen von Firewalls unterscheidet man dem Verfahren nach die Datenpaket-Filterung, das Circuit-Relay und den Application-Gateway. Alle drei Funktionalitäten setzen auf unterschiedlichen Schichten auf und verbinden das Internet mit dem Landeskirchennetz.	Einsatz: Als Protokolle, die Firewalls zu externen Netzen ohne weiteres Sicherheitskonzept mit Standard-Sicherheitsfunktionen passieren lassen, sind zugelassen: • HTTPS • SMTP • LDAP • DNS. Dies sind auch die Protokolle des standardisierten Firewalls. Die Nutzer von Firewalls müssen Restrisiken einplanen.

4. Erstellung von Sicherheitskonzepten

Standard	Beschreibung/Definition	Einsatz/Begründung
Allgemein	Fundstelle: IT-Grundschutzhandbuch des BSI, Ausgabe 2004 Bei einem Schutzbedarf "niedrig bis mittel" reichen i. d. R. die Standardsicherheitsmaßnahmen des IT-Grundschutzhandbuchs aus. Bei einem Schutzbedarf "hoch bis sehr hoch" kann es sinnvoll sein zu prüfen, ob die Standardsicherheitsmaßnahmen durch höherwertige, meist jedoch auch kostspieligere, IT-Sicherheitsmaßnahmen ergänzt oder ersetzt werden müssen. Welche zusätzlichen Maßnahmen geeignet sind, kann nach Durchführung des Basis- Sicherheitschecks nach IT-Grundschutz mittels einer ergänzenden Sicherheitsanalyse (z. B. Risikoanalyse) festgestellt werden.	Einsatz: IT-Systeme der Landeskirche im Rahmen des IT-Konzepts haben in der Regel differenzierten Schutzbedarf. Deshalb ist das IT-Grundschutzhandbuch anzuwenden.
Schutzbedarfsfeststellung	Ausgehend von den 3 Grundbedrohungen 1. Verlust der Unversehrtheit 2. Verlust der Vertraulichkeit 3. Verlust der Verfügbarkeit wird für das untersuchte IT-System ermittelt, welche Schäden bzw. Folgen durch Sicherheitsverletzungen entstehen würden. Beispiele: • Verstöße gegen Gesetze, Vorschriften, Verträge • Beeinträchtigung des informationellen Selbstbestimmungsrechts • Beeinträchtigung der persönlichen Unversehrtheit • Beeinträchtigung der Aufgabenerfüllung • Finanzielle Auswirkungen. Daraus ergibt sich der konkrete Schutzbedarf.	Einsatz: IT-Anwendungen der Landeskirche im Rahmen des IT-Konzepts haben in der Regel differenzierten Schutzbedarf. Deshalb ist das IT-Grundschutzhandbuch anzuwenden.
Risikoanalyse	Die Risikoanalyse setzt immer auf einer Schutzbedarfsfeststellung auf (siehe IT-Grundschutzhandbuch). Wird nach Durchführung des Basis-Sicherheitschecks nach IT-Grundschutz der Bedarf nach einer erweiterte Sicherheitsanalyse erkannt, empfiehlt es sich, zunächst eine Bedrohungsanalyse durchzuführen, bei der die bedrohten Objekte des IT-Systems und alle vorstellbaren Bedrohungen (Schwachstellenanalyse) in angemessenem Umfang ermittelt werden.	Einsatz: IT-Anwendungen der Landeskirche im Rahmen des IT-Konzepts haben in der Regel differenzierten Schutzbedarf. Deshalb ist das IT-Grundschutzhandbuch anzuwenden.

Standard	Beschreibung/Definition	Einsatz/Begründung
	Die Objektbildung kann z. B. nach folgenden Gruppen gegliedert werden: 1. Infrastruktur 2. Hardware 3. Software 4. Datenträger 5. Anwendungsdaten 6. Kommunikation 7. Personen Wobei zweckmäßigerweise alle wesentlichen Prozesse und Datenströme zerlegt und die Teile auf Manipulationsmöglichkeiten hin untersucht und bewertet werden. Bei der anschließenden Risikobetrachtung werden die Schadenswerte/ Häufigkeiten der Bedrohungen für die Objekte bewertet und daraus das differenzierte Sicherheitsrisiko R (R = p*S; p= Wahrscheinlichkeit für einen Schaden, S= mittlerer Schaden) ermittelt.	
Sicherheitskonzept	Hier werden die Maßnahmen gegen die Bedrohungen ausgewählt und ihre Wirkungen beurteilt. Dabei ist zu entscheiden, welche Maßnahmen angemessen sind (Kosten-Nutzen-Betrachtung) und welches Restrisiko tragbar ist.	

5. Internet-Anschluss

Standard	Beschreibung/Definition	Einsatz/Begründung
Landeskirchlicher Standard	Netze einer Kirchlichen Verwaltung dürfen nur auf der Grundlage eines detaillierten Sicherheitskonzepts an das Internet angeschlossen werden. Benutzer des OKR-Netzes können über ein logisches Intranet mittels zentralen Internet-Zugangs des OKR, der durch ein Firewallsystem und einen zentralen Virenscanner geschützt ist, an das Internet angeschlossen werden. Die Dienststellen, die einen Internet-Zugang in ihrem LAN bereitstellen, müssen sicherstellen, dass dadurch keine Störungen, Eindringversuche oder sonstige Risiken in irgendeiner Benutzergruppe des Netzes entstehen. Bei Internet-Anschlüssen ist zudem sicherzustellen, dass durch klare Zuständigkeitsregelungen eine laufende tatsächliche Kontrolle und Aktualisierung der Technik sichergestellt ist. Datenbestände, die dem Risiko des Internetzugangs nicht ausgesetzt werden dürfen, sind durch physische Trennung oder Verschlüsselung (z. B. durch PGP) zu schützen.	Einsatz: IT-Systeme müssen so betrieben werden, dass sie andere Systeme nicht stören oder an sie Störungen weiterleiten. Durch den Betrieb eines zentralen und leistungsfähigen Internet-Anschlusses über einen mit modernen Tools professionell administrierten Firewall werden Kosten und Sicherheitsrisiken minimiert.

6. Sicherheit bei Telearbeit und bei Arbeit außerhalb der Dienststelle

Die Standards des IT-Konzepts berücksichtigen die personalrechtlichen Fragen, die Organisation der Telearbeit und Definitionen zur Telearbeit nicht, sondern beschränken sich auf Empfehlungen zu Sicherheitsmaßnahmen, die bei der Nutzung privater oder dienstlicher Geräte für dienstliche Zwecke notwendig werden. Deshalb werden die Bestimmungen in der Arbeitsrechtlichen Regelung zur Telearbeit –Dienstzimmer im Privatbereich– Beschluss der Arbeitsrechtlichen Kommission vom 8.Dezember 2006 (Abl. 62 S. 328) durch die hier genannten Sicherheitsmaßnahmen ergänzt.

Aus Sicht des IT-Konzepts kann den Bediensteten grundsätzlich erlaubt werden, mit privaten Geräten sicherheitsmäßig unbedenkliche Verarbeitungsvorgänge durchzuführen. Solche Vorgänge sind z. B. dienstliche Anrufe über private Handys, dienstlich relevante SMS über private Handys, Erstellung von Vorträgen und Vortragsfolien mit privatem PC, sofern keine sensiblen Informationen übertragen werden und durch den Datenaustausch mit dem privaten Gerät keine Gefährdung dienstlicher Informationstechnologie entsteht.

CITRIX-Portal (siehe Kapitel III Netz- und Kommunikationsstrukturen, Punkt 9. Portal, Seite 20).

Darüber hinaus gilt, dass der Nutzer privater Informationstechnologie in der Lage sein muss, die dabei anfallenden technischen Vorgänge bezüglich des Risikos zu bewerten.

Standard	Beschreibung/Definition	Einsatz/Begründung
Handys, Personal Digital Assistants, Subnotebooks und Smartphones sowie Notebooks	Sicherheitsfragen bestehen bei der genannten Gerätegruppe je nach Ausstattung und Leistungsfähigkeit der Geräte insb. bezüglich • der Vertraulichkeit bei der Verarbeitung (z. B. Vertraulichkeit von Adressverzeichnissen, Personenlisten, Vermerken z. B. im Zusammenhang mit einer Vergabe, Arbeit an öffentlichen Plätzen wie z. B. bei einer Dienstreise) • der Abschottung gegenüber Dritten (z. B. beim Vergessen eines Geräts im Zug, beim Hinterlassen eines Geräts im Hotelzimmer während der Einnahme von Mahlzeiten) • der Aktualisierung von Verzeichnissen und Dokumentenablagen (z. B. Vermeiden von falschen Verarbeitungsvorgängen) • Verhindern einer Benutzung durch Dritte (z. B. sollen Diebe eine SIM-Card oder ein Notebook nicht oder zumindest nicht ohne weiteres nutzen können) • Verhindern von zufälligen Fehlern (z. B. Bedienungsfehler).	Dienstlich bereitgestellte Geräte sind immer durch ein Passwort zu sichern. Auf einem privaten Gerät dürfen keine dienstlichen Daten verarbeitet werden. Wenn regelmäßig vertrauliche oder sensible Informationen gespeichert oder sonst verarbeitet werden und das Gerät von Dritten unbefugt benutzt werden könnte, müssen die schützenswerten Daten nach dem Stand der kommerziellen Technik verschlüsselt werden.
Telearbeitsplätze ohne direkten Zugriff auf das dienstliche Bürokommunikationssystem	Soweit kein zwingender Bedarf vorhanden ist, werden Telearbeitsplätze aus Sicherheits- und Kostengründen nur über E-Mail-Verbindungen mit dienstlichen Bürokommunikationssystemen vernetzt. Solche Telearbeitsplätze haben i. d. R außerdem Zugang zum Internet. Telearbeiter müssen beim Einsatz der Telearbeitstechnik die Wirtschaftlichkeit ständig berücksichtigen.	Wenn vertrauliche oder sensible Informationen über das Internet übertragen werden, sind die Daten bei der Übertragung zu verschlüsseln. Der Telearbeiter muss, wenn er andere Internet-Dienste als E-Mail nutzt, die Risiken kennen und sicherstellen, dass durch seine Internet-Nutzung keine Risiken für die dienstliche Informationstechnologie entstehen. Eine Authentifikation über Passwort ist vorzusehen. Die allgemein üblichen Passwort-Regelungen (vgl. z. B. Empfehlungen des Datenschutzbeauftragten im Internet) sind umzusetzen. Der Telearbeiter muss den Datenbestand auf seinem PC so verwalten, dass er alle Anforderungen der Datenschutzvorschriften (insb. Richtigkeit, Auskunft über die gespeicherten

Standard	Beschreibung/Definition	Einsatz/Begründung
		Daten und die benutzten Verfahren, Übermittlungskontrolle, Löschung z. B. bei veralteten Daten oder bei Fehldrucken) erfüllt.
Telearbeitsplätze mit direktem Zugriff auf das dienstliche Bürokommunikationssystem	Bei diesen Telearbeitsplätzen sind neben den o.g. Sicherheitsmaßnahmen noch Maßnahmen zum sicheren Zugang zu dem dienstlichen Bürokommunikationssystem zu ergreifen.	Der Zugang zum dienstlichen Bürokommunikationssystem muss zusätzlich zu den o. g. noch folgende Anforderungen erfüllen: • Sichere Authentifikation des Telearbeiters • Aktivierung der Abschottungsregeln im dienstlichen Bürokommunikationssystem beim Telearbeitszugang, die beim Zugang im Büro gelten • Verschlüsselung des Datenverkehrs, falls ausländische Netze genutzt werden könnten • Automatische Erkennung von Kommunikationsstörungen mit automatischem Abmelden des Telearbeiters. Einsatz: Im OKR wird das CITRIX-Portal (s.III.9.1) als Zugang angeboten.

7. Zugriffssicherung/Berechtigungsprüfung

Standard	Beschreibung/Definition	Einsatz/Begründung
Basis-Authentifizierung	Dieses Standard-Verfahren zur Absicherung von Benutzerzugriffen auf Serveranwendungen beruht auf der Prüfung von Benutzername und Passwort. In Intranets mit heterogenen Client-Server-Umgebungen und im Internet werden diese Login-Parameter unverschlüsselt im Netz übertragen. Daraus ergibt sich ein erhöhtes Sicherheitsrisiko. In homogenen Client-Server-Umgebungen wie z. B. Windows erfolgt diese Übertragung teilweise verschlüsselt.	Einsatz: Regelmäßig bei Grundverfahren der einheitlichen IT-Infrastruktur und bei Netzwerk- Anwendungen innerhalb des OKR-Intranets. Dieses Verfahren ist als Sicherheitsmaßnahme im Internet grundsätzlich nicht geeignet.
Höherwertige Authentifizierung Internet-Standard	Dieses Verfahren unterstützt sowohl die Authentifizierung als auch die gesicherte Datenübertragung. Für eine sichere und vertrauliche Kommunikation über öffentliche Netze sind folgende Lösungen einzusetzen: • Kommunikationsebene: Basis SSL V.3 bzw. TLS V1.0 ggf. mit Client-Authentifizierung ; SSL/TLS nutzt die Public Key Kryptografie zur Authentifizierung und die Secret Key Kryptografie zur Verschlüsselung der auszutauschenden Nachrichten; die Schlüsselzertifikate (Client und Server) müssen von Zertifizierungsinstanzen stammen, die von Clients und Server anerkannt werden. • Anwendungsebene: Einmalpasswörter in Verbindung mit Authentifizierungsservern ermöglichen ein sicheres Login. Einmalpasswörter werden für jeden Loginvorgang auf speziell programmierten Token neu erzeugt. Für den sicheren Datenaustausch sorgen dann Verschlüsselungsprogramme.	Einsatz: Insbesondere wenn Zugriffe über fremde Netze erfolgen oder wenn ein Firewall einfacher gestaltet werden soll, ist eine Sicherung über die SSL-Mechanismen geboten.

8. Kryptografische Verfahren

8.1. Kryptografische Standards

Schlüssellänge und Verfahren sind bei den kryptografischen Standards zusammenhängend zu betrachten.

Standard	Beschreibung/Definition	Einsatz/Begründung
Symmetrische Verfahren		Einsatz: Typisches Anwendungsgebiet für symmetrische Algorithmen ist die vertrauliche Speicherung von Daten auf lokalen Laufwerken (z. B. Festplatten, Disketten) oder auf einem Server
DES ANSI-Standard	Fundstelle: ANSI (American National Standards Institute) X3.92-1981 (Data Encryption Standard) Der DES-Algorithmus (für Anwendungs- und Kommunikationsebene) ist ein Blockchiffrierer, der unter Verwendung eines 64 Bit Schlüssels (56 Bits signifikant, 8 Paritätsbits) 64 Bits Klartext in 64 Bits Schlüsseltext transformiert	Einsatz: Vom Einsatz wird abgeraten Begründung: DES ist zwar weit verbreitet, allerdings auf Grund der geringen Schlüsselgröße von 56 Bits umstritten.
3DES NIST-Standard	Fundstelle: NIST -Standard (National Institute of Standards and Technology) Triple-DES (3DES) erhöht die Sicherheit des normalen DES-Verfahrens, indem die Daten mit doppelter (112 Bit) oder dreifacher (168 Bit) Schlüssellänge verschlüsselt werden.	Einsatz: Stärkere Verschlüsselung, deshalb Einsatz bei höherem Sicherheitsbedarf sinnvoll.
IDEA	IDEA (International Data Encryption Standard) ist ähnlich wie DES ein symmetrischer IDEA (International Data Encryption Standard) ist ähnlich wie DES ein symmetrischer Verschlüsselungs-Algorithmus. IDEA verwendet eine Schlüssellänge von 128 Bit.	Wie 3DES
AES	AES (Advanced Encryption Standard, auch Rijndael genannt) soll den DES Standard ablösen. Das National Institute of Standards and Technology (NIST) hat AES am 26.11.2001 zum Standard erklärt. Erste Produkte sind verfügbar. Geforderte Schlüssellängen im AES-Standard sind 128, 192 und 256 Bit.	Einsatz: Da inzwischen in der Presse erste Berichte zu erfolgreichen Angriffen auf AES erschienen sind, sollten vor einem Einsatz noch weitere Erfahrungen abgewartet werden.
Asymmetrische Verfahren		
RSA	Fundstelle: R. Rivest, A. Shamir, L. Adleman: *A method for obtaining digital signatures and public key cryptosystems*, *Communications of the ACM*, Jahrgang 21, Nr. 2 (1978) RSA basiert auf dem Schlüsselaustausch-Algorithmus von Diffie-Hellmann (1976), der die Grundlage für die Public Key Kryptografie darstellt. Während symmetrische Verfahren darauf beruhen, dass Daten und Informationen mit demselben Schlüssel ver- und entschlüsselt werden, wird beim asymmetrischen Verfahren ein Schlüsselpaar, bestehend aus dem geheimen (private Key) und dem öffentlichen Schlüssel (public Key) verwendet. Daten, die mit einem öffentlichen Schlüssel verschlüsselt werden, können nur mit dem zugehörigen geheimen Schlüssel entschlüsselt werden und umgekehrt. Die Berechnung des geheimen Schlüssels zu einem vorgegebenen öffentlichen Schlüssel beruht beim RSA-Verfahren auf der Faktorisierung großer Zahlen, d.h. der Zerlegung in ihre Primfaktoren. Das RSA-Verfahren ist auch die Grundlage für die elektronische Signatur, bei der die zu signierenden Daten zunächst mit einem geeigneten Zufallsverfahren komprimiert werden	Einsatz: Regelmäßig im Zusammenhang mit allen Verfahren zur • Ende-zu-Ende- Verschlüsselung der elektronischen Post • elektronischen Signatur Begründung: RSA ist heute Standard für die asymmetrische Verschlüsselung mit und ohne Chipkarten bis Schlüssellangen von ca. 2048 Bits. Für größere Schlüssellängen wird das Verfahren bei der elektronischen Signatur und Entschlüsselung sehr aufwendig. Deshalb ist hier die Elliptic Curve Cryptography (ECC) als Alternative zu RSA sehr stark im Kommen.

Standard	Beschreibung/Definition	Einsatz/Begründung
	und dieses Komprimat dann mit dem geheimen Schlüssel des Signierenden verschlüsselt werden. In Verbindung mit einer durch ein Zertifikat erfolgten Personalisierung des zugehörigen öffentlichen Schlüssels kann der Nachweis der Unversehrtheit der signierten Daten und der Authentizität des Signierenden erbracht werden.	
DSS	Fundstelle: NIST FIPS Publication 186: *Digital Signature Standard*, Mai 1994: 1984 hat El'gamal einen zu RSA alternativen Signaturalgorithmus vorgeschlagen. Eine Variante dieses El'gamal-Verfahrens ist der 1991 von NIST publizierte Standard DSS, der den Digital Signature Algorithmus (DSA) spezifiziert. Neue Varianten des DSA basieren auf Punktegruppen elliptischer Kurven.	Einsatz: Ggf. künftig als Alternative zu RSA für die elektronische Signatur zulässig Begründung: Veröffentlichung der RegTP über "Geeignete Kryptoalgorithmen", BundesAnz. Nr. 158 S. 18 562 vom 24.08.2001
Hybrid Verfahren	Kombination aus symmetrischen (in der Regel DES, 3DES) und asymmetrischen Verfahren (RSA) (siehe S/MIME und PGP, Nr. 9.6.2) Hierbei wird die Nachricht vom Absender zunächst mit einem zufällig generierten Schlüssel symmetrisch verschlüsselt. Der verwendete Schlüssel wird dann mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und zusammen mit der symmetrisch verschlüsselten Nachricht übermittelt.	Einsatz: Regelmäßig bei allen Verfahren zur Ende-zu-Ende-Verschlüsselung der elektronischen Post.

8.2. Verschlüsselungs-Software

Standard	Beschreibung/Definition	Einsatz/Begründung
Verschlüsselung auf Kommunikationsebene		
SSL V. 3 IETF-Standard	SSL ist eine Entwicklung von Netscape für die sichere Datenkommunikation im WWW, kann jedoch auch für andere Anwendungsprotokolle der TCP/IP-Familie wie Telnet, FTP eingesetzt werden. SSL wird von allen gängigen Internet-Browsern und Server-Produkten unterstützt. Die Spezifikation zu SSL wurde Ende 1995 der Internet Engineering Task Force (IETF) zur Standardisierung vorgelegt. Aktuell ist die Version 3.2 von November 1996, die als Internet-Draft vorliegt.	Einsatz: • für die Sicherung besonderer Inhalte im Netz des OKR. Im Intranetverbund ist die sichere US-Exportversion ausreichend. Das Root-Zertifikat (=Zertifizierungsstellen-Zertifikat) wird bereitgestellt Begründung: Bestandteil der einheitlichen IT-Infrastruktur
TLS V1.0	TLS (Transport Layer Security) ist eine Weiterentwicklung von SSL V.3. Die Protokoll-Version 1.0 wurde 1999 veröffentlicht (RFC 2246). Im Gegensatz zu SSL V.3 ist bei TLS V1.0 die Server-Authentifikation optional. Zur Vermeidung von sog. "man-in-the-middle"-Attacken sollte auf diese Funktion jedoch nicht verzichtet werden.	
IPSec IETF-Standard	Bezeichnung für einen Standard, der Verschlüsselung und Authentifizierung für IP-Netze auf der Vermittlungsschicht regelt IPSec ist sowohl für IPv4 als auch für IPv6 definiert. Die Sicherheit gewährleistet IPSec über einen Authentifizierungsheader und ein Sicherheitseinkapselungspaket (Encapsulating Security Payload -ESP-). Im ESP sind die Nutzdaten des Paketes oder ein komplettes Paket (Tunneling) mit einem symmetrischen Algorithmus (DES, 3DES oder IDES) verschlüsselt. IPSec steht in den heutigen Routern z. B. von CISCO und in Verschlüsselungsboxen z. B. von Utimaco, Biodata zur Verfügung. Innerhalb des FreeS/WAN Projektes gibt es zwei frei verfügbare und durch Exportrestriktionen nicht reglementierte	Einsatz: für die Realisierung von VPN-Lösungen und Tunneling z. B. • zur besonderen Sicherung von Benutzergruppen (z. B. PersonalOffice-Anwender) oder • anstelle von Verschlüsselungslösungen auf Anwendungsebene (z. B. SSL)

Standard	Beschreibung/Definition	Einsatz/Begründung
	Versionen von IPSec für Linux: • Pluto • JI's IPSec von John Ioannidis.	
IKE IETF-Standard	IKE ist ein von der Firma Cisco und der IETF erarbeiteter Protokollrahmen zur Verwaltung von Security Associations in IPSec. ISAKMP (Internet Security Association Key Management Protocol) ist nur ein Rahmenwerk. Eine konkrete Umsetzung ist IKE. Internet Key Exchange (IKE) ist ein Protokoll, das der Verwaltung von Sicherheitskomponenten innerhalb von mit IPSec realisierten VPN dient. IKE wird benötigt, da IPSec die zur Verschlüsselung notwendigen Informationen (Algorithmus, Schlüssel, Gültigkeitsdauer etc.) nicht selbst überträgt, sondern sie aus einer lokalen Sicherheits-Datenbank übernimmt.	Einsatz: Der Einsatz ist in VPN Lösungen zum Austausch von Sicherheitsinformationen erforderlich.
Verschlüsselung auf Anwendungsebene		
Pretty Good Privacy de-facto- Standard	PGP (Pretty Good Privacy), Hybridverfahren aus RSA und IDEA, also eine Kombination aus symmetrischen mit asymmetrischen Verfahren, Public-Key-Verfahren zur Verschlüsselung von Daten PGP ist bei privater Nutzung lizenzkostenfrei; die Nutzung innerhalb der Verwaltung ist jedoch lizenzpflichtig. Für PGP gibt es Plug-Ins sowohl für MS-Outlook als auch für die Mail-Clients der Standard-Web-Browser (MS Outlook-Express, Netscape Messenger). Internet Freeware/ Shareware kann dienstlich nicht eingesetzt werden (vgl. Nr. 9.2). Alternativ kann das vom BSI geförderte GNU Privacy Guard (GnuPG) eingesetzt werden. Allerdings sind GnuPG und PGP derzeit noch nicht vollständig miteinander interoperabel.	Einsatz: soweit zweckmäßig zur • Ende-zu-Ende-Verschlüs-selung der elektronischen Post mit Externen, soweit nicht die gesetzeskonforme elektronische Signatur anzuwenden ist • zum Schutz bei Internetanschlüssen für die Verschlüsselung von lokal zu speichernden Dateien Begründung: Bestandteil der einheitlichen IT-Infrastruktur
MailTrusT (MTT) Nationaler Standard	Standard des Industrieverbands Teletrust e.V., dem alle wichtigen deutschen Hersteller kryptografischer Softwareprodukte für die Ende-zu- Ende-Verschlüsselung angehören MTT setzt auf dem Standard PEM (Privacy Enhanced Mail) auf. Die Version 2 ist weitgehend mit S/MIME V3 identisch und enthält unter anderem: • S/MIME als Austauschformat • Zertifikatsformate nach X.509 V. 3. Der Einsatz mit Mail-Clients von Web- Browsern (z. B. Outlook Express, Netscape Messenger) ist derzeit nur beschränkt möglich. Die Interoperabilität der Produkte auf der Basis von MTT V.2 wurde im Rahmen des Sphinx-Projektes des Bundes untersucht. Um Interoperabilität zwischen unterschiedlichen PKI-Lösungen für die Verschlüsselung (nach MTT V. 2) und die - insbesondere qualifizierte - elektronische Signatur (entsprechend den "Industrial Signature Interoperability Specifications" [ISIS V. 1.2], einem von der Arbeitsgemeinschaft der deutschen Trust Center [AGTC] verabschiedeten Standard) zu erzielen, wurde mit ISIS-MTT ein gemeinsamer Standard entwickelt, der als Version 1.02 seit 19.07.2002 vorliegt. Trust Center bieten inzwischen spezielle Dienstleistungen nach dem ISIS-MTTStandard an (z. B. Zeitstempeldienst der Fa. TTeleSec). Nach den Erfahrungen von Fa. Datev und Fa. secaron unterstützen die auf dem Markt verfügbaren Microsoft-Anwendungen Zertifikate gemäß ISIS-MTT-Spezifikation.	Einsatz: In der landeskirchlichen Verwaltung können im Rahmen dereinheitlichen Bürokommunikation solche Produkte für die Ende-zu-Ende-Verschlüsselung der elektronischen Post eingesetzt werden, die dem Mail-TrusT-Standard V. 2 und ISIS-MTT V 1.02 entsprechen. Danach ist diese Verschlüsselungstechnik in der Regel • nicht einzusetzen beim Versand im LAN • einzusetzen beim Versand über das Internet oder andere unbekannte Netze, sofern im Einzelfall z. B. auf Grund der geringen Schutzbedürftigkeit der versendeten Daten nicht anders entschieden wird. Begründung: Bestandteil der einheitlichen IT-Infrastruktur. ISISMTT wird zu gegebener Zeit aufgenommen.
S/MIME Firmen-Standard	S/MIME basiert ebenfalls auf dem asymmetrischen Schlüsselsystem. Im direkten Vergleich zu PGP ergeben sich folgende Unterschiede: • Im Gegensatz zu PGP bedarf S/MIME immer des Einsatzes von Schlüsselzertfikaten, die von einem Trust Center ausge-	Einsatz: Für die Verschlüsselung von E-Mails ist S/MIME mit einem starken Verschlüsselungsalgorithmus (mindestens 112 Bits Schüssellänge) einzusetzen.

Standard	Beschreibung/Definition	Einsatz/Begründung
	stellt werden. • Weiterhin wird, im Unterschied zu PGP, bei der elektronischen Signatur einer E-Mail immer zwingend das Zertifikat des öffentlichen Schlüssels entsprechend X 509 V. 3 angehängt. • S/MIME garantiert durch die Mail-Struktur nach PKCS # 7, dass eine an mehrere Empfänger (z. B. Verteilerliste) gerichtete verschlüsselte Mail für alle Empfänger dasselbe Format besitzt.	(vgl. Regelungen zu MTT) Begründung: Bestandteil der einheitlichen IT-Infrastruktur

8.3. Standard für Schlüssel-Zertifikate

Standard	Beschreibung/Definition	Einsatz/Begründung
X.509 ITU-Standard	Fundstelle: X.509 ist ursprünglich ein IEEE-Standard, der von der ITU übernommen wurde. Der gebräuchliche Standard für digitale Zertifikate ist der ITU Standard X.509v3. X.509 setzt auf den Namenskonventionen des Verzeichnis-Standards X.500 auf. X.509 definiert den Aufbau und Inhalt (Attribute) für die Zertifikate öffentlicher Schlüssel im Rahmen einer so genannten PKI (Public Key Infrastructure). Ein solches Zertifikat enthält neben dem öffentlichen Schlüssel des Eigentümers Angaben zur Identifikation (Name, ggf. Wohnort, etc.) des Eigentümers und zum Zertifikat selbst (Name der Zertifizierungsstelle, Gültigkeitsdauer des Zertifikats, X.509-Version, Zertifikats-Nummer, etc). Darüber hinaus enthalten Zertifikate i.d.R. eine elektronische Signatur der Zertifizierungsstelle. X.509v3 unterscheidet sich von seinen Vorgänger- Versionen insbesondere dadurch, dass weitere Angaben zum Eigentümer (z. B. Geburtsdatum) oder zum Zertifikat als sog. Extensions hinzugefügt werden können.	Einsatz: Regelmäßig beim Einsatz von asymmetrischen oder hybriden Verschlüsselungsverfahren und bei der elektronischen Signatur. Begründung: Wird eine Institution oder Person zertifiziert, so geschieht dies über die eindeutige Bindung ihres öffentlichen Schlüssels an ihren Namen und weitere Attributinformationen, die das zu zertifizierende Subjekt charakterisieren. Eine Zertifizierungsstelle bestätigt als vertrauenswürdiger Dritter diese Bindung mit elektronischer Signatur. Im Netz des OKR werden die Zertifikate in ein Einheitliches Benutzerverzeichnis eingestellt und können von dort z. B. per LDAP oder http abgerufen werden.

8.4. PKI-Konzept

Um die rechtlichen Anforderungen der Datenschlüsselungsverordnung umzusetzen wurde im Evangelischen Oberkirchenrat eine PKI (Public Key Infrastructure) auf Basis von S/MIME aufgebaut.

Für das Ausstellen und Verteilen der Zertifikate steht im Evangelischen Oberkirchenrat ein Server als Zertifizierungsstelle zur Verfügung. Hier können Zertifikate angefordert und abgeholt werden. Die Zertifikate werden dann auf dem lokalen Rechner gespeichert und stehen damit zur Verfügung. Auch die öffentlichen Schlüssel evtl. E-Mail-Partner können von diesem Server abgeholt werden.

Der Zugang zum Zertifikatsserver erfolgt über die Internet-Adresse: http://pki.elk-wue.de.

Standard	Beschreibung/Definition	Einsatz/Begründung
PKI für die E-Mail-Verschlüsselung	Für eine verschlüsselte Übertragung benötigen Sender und Empfänger ein digitales Zertifikat. Ein digitales Zertifikat ist ein Datensatz, der Informationen über den Namen des Inhabers, dessen öffentlichen Schlüssel, die E-Mail Adresse, eine Seriennummer, eine Gültigkeitsdauer und den Namen der Zertifizierungsstelle enthält. Eine digitale Signatur schützt diesen Datensatz gegen Veränderung. Jeder Teilnehmer an der Verschlüsselung hat einen "Öffentlichen Schlüssel", den jeder bei einer im Netz zugänglichen Stelle abholen kann und der nur zur Verschlüsselung an ihn gerichteter Nachrichten dient. Der Absender verschlüsselt E-Mails mit dem öffentlichen Schlüssel des Empfängers und versendet sie. Nur der Empfänger kann verschlüsselte E-Mail mit seinem privaten Schlüssel entschlüsseln und damit lesen.	Einsatz: Um den dienstlichen E-Mail-Verkehr zwischen Oberkirchenrat, den Kirchlichen Verwaltungsstellen, den Prälaturen, Dekanatämtern und Pfarrämtern in verschlüsselter Form abwickeln zu können, wurde im Evangelischen Oberkirchenrat die Infrastruktur auf der Basis des S/MIME Standards (Secure / Multipurpose Internet Mail Extension, Sicherheits-Erweiterung der E-Mail-Kommunikation) eingerichtet. Für den verschlüsselten Datenverkehr zwischen weiteren Datenstellen kann auch PGP (Pretty Good Privacy, bekannte Verschlüsselungssoftware für Einzelrechner) eingesetzt werden.

Anlagen

Anlage 1: Hardware und Systeme für externe Dienststellen

Diese Anlage enthält Empfehlungen zur Hardware- und zur Netz-Konzeption für kleine und mittlere Einrichtungen (in Ergänzung zum IT-Konzept). Sie wurde erstellt unter Berücksichtigung der im IT-Konzept ausführlich beschriebenen Standards, beschränkt sich aber in den Ratschlägen für die Umsetzung auf die für kleinere und mittlere Dienststellen in erster Linie wichtigen praktischen Erfahrungen.

Für die Umsetzung wurde von drei Kategorien ausgegangen:

1. Dienststellen mit Einzel-PCs
2. Dienststellen mit Vernetzung und bis zu 5 PCs
3. Dienststellen mit Vernetzung und über 5 PCs

Anmerkung: Windows Vista und Office 2007 sind neue Softwareprodukte der Firma Microsoft. Gegenwärtig unterstützt Windows Vista noch nicht alle Anwendungsprogramme unserer Landeskirche (z. B. Kifikos). Insbesondere im Modul PowerPoint und im Makrobereich sollte zurzeit. mit Kompatibilitätsproblemen gerechnet werden, die sich durch spezielle Tools von MS nicht vollständig beseitigen lassen. Aus diesen Gründen wird gegenwärtig nicht empfohlen, Windows Vista und Office 2007 umgehend einzusetzen. Es wird an dieser Stelle ausdrücklich darauf hingewiesen, dass es sich hierbei um eine vorläufige Empfehlung handelt.

1. Dienststellen mit 1-2 Einzel-PCs:

Gerät/Ausstattung:	Bemerkung:
PC mit: • Prozessor Intel/AMD mit ca. 3GHz bzw. Dual Core Prozessoren • Hauptspeicher: 512 - 1024 MB • Festplatte: 80 – 250 GB • CD/DVD-Brenner • Microsoft Windows XP Professional • Microsoft Office XP oder 2003	Für die normale Bürotätigkeit reicht ein PC im mittleren Preissegment aus. Höhere Rechenleistung ist nur notwendig wenn häufig aufwendige Bildbearbeitung gemacht werden soll. Höchste Rechenleistung ist meist überproportional teuer. Für die Datensicherung bietet sich je nach Menge der Daten ein DVD oder CD-Brenner an, da diese eine einfache Handhabung sowohl bei Sicherung als auch bei der Wiederherstellung der Daten bieten. Als Betriebssystem sollte MS Windows XP Professional eingesetzt werden, da dieses stabil läuft und auch relativ viele Programme dafür verfügbar sind. Außerdem unterstützt der OKR momentan nur MS Win XP Professional (oder ältere MS Betriebssysteme) für seine Programme. Im Gegensatz zur Home-Variante ermöglicht Professional differenziertere Sicherheitseinstellungen und ermöglicht später auch eine professionelle Vernetzung. Für die Bürokommunikation empfiehlt es sich MS Office XP oder 2003 zu nehmen, da dies einen problemlosen Austausch von Dokumenten mit vielen anderen Dienststellen ermöglicht – MS-Office ist derzeit Defacto Standard.
Internet-Zugang • ISDN-Karte: z. B. AVM Fritz!Card (für Internetanbindung); • Netzwerkkarte und DSL-Modem für DSL-Internetzugang	Für den Internetzugang stehen als Alternativen ISDN oder DSL zur Verfügung. ISDN ist zu empfehlen wenn nur gelegentlich Informationen aus dem Internet abgerufen werden. DSL rentiert sich bei Online-Zeiten von mehr als ca. 40 Std./Monat oder großen Download-Mengen, da hierfür sog. Flatrates verfügbar sind.
Funk-LAN	Funk-LANs bzw. Wireless LANs (WLANs) bieten die Möglichkeit, mit geringem Aufwand drahtlose Netze aufzubauen Aufgrund der bequemen Einrichtung der WLAN-Netze, der Übertragung auch über Grundstücksgrenzen hinaus und evtl. falsch (vor-) konfigurierter Geräte müssen mindestens folgende Datenschutz- und Sicherheitsmaßnahmen ergriffen werden: • Netzwerkname (SSID) unterdrücken • WPA Verschlüsselung einschalten (langes Kennwort)

Gerät/Ausstattung:	Bemerkung:
	• Zugangsfilter im Access Point einrichten (MAC-Adressen der Teilnehmer) Weitere Maßnahmen wie VPN einrichten oder DHCP deaktivieren, werden empfohlen (Näheres siehe Informationsschrift "Sicherheit im Funk-LAN" des BSI, 2003).
E-Mail	Für E-Mail-Kommunikation stehen derzeit mehrere Programme zur Verfügung. Outlook Express ist kostenlos im Betriebssystem enthalten, während Outlook meist mit dem Office-Paket geliefert wird. Alternativ gibt es noch Mozilla Thunderbird.
Virenschutz + Personal-Firewall	Unbedingt notwendig ist ein Virenschutz der regelmäßig (am besten automatisch) aktualisiert wird. Alternativ zur Firewall von Windows kann eine Personal-Firewall verwendet werden, die differenzierte Einstellungen ermöglicht.
Drucker: Tintenstrahldrucker; alternativ Laserdrucker	Welche Druckerart man wählt hängt von der Art und der Menge der zu druckenden Dokumente ab. Tintenstrahldrucker sind in der Anschaffung günstig und bieten die Möglichkeit, farbige Ausdrucke zu machen. Allerdings sind die Druckkosten pro Seite relativ teuer, speziell bei Farbdrucken. Sie eignen sich somit für gelegentliche Ausdrucke mit farbigen Elementen. Laserdrucker bieten erst bei teureren Modellen Farbdrucke. Die kleineren Monochrom-Modelle eigenen sich vor allem für kleine bis mittlere Druckvolumina, die keinen Farbdruck erfordern. Die Kosten pro Seite sind deutlich geringer als bei Tintenstrahldruckern.
Scanner	In der Regel sind die meisten Modelle für den Bürogebrauch geeignet. Sollen aber gelegentlich Dias gescannt werden, muss ein Modell gewählt werden, das eine sog. Durchlichteinheit hat.
Zugang zum OKR-Netz: Zugangskennungen	Auf den Rechnern des OKR werden neben der Bürokommunikation eine Reihe weiterer Anwendungen im Bereich Personalwesen, Finanzwesen u. a. angeboten. Der Zugang erfolgt üblicherweise über das Internet und das Produkt Citrix, das auf dem lokalen PC installiert wird. Die Zugangskennung vergibt das Referat IT.

2. Dienststellen mit bis ca. 5 PCs:

Gerät:	Bemerkung:
PC(s) mit: • Prozessor Intel/AMD mit ca. 3GHz bzw. Dual Core Prozessoren • Hauptspeicher: 512 - 1024MB • Festplatte: 80 – 250 GB • CD/DVD-Brenner • Netzwerkkarte für Peer-to-Peer-Vernetzung • Microsoft Windows XP Professional • Microsoft Office XP oder 2003	Für die normale Bürotätigkeit reicht ein PC im mittleren Preissegment aus. Höhere Rechenleistung ist nur notwendig wenn häufig aufwendige Bildbearbeitung gemacht werden soll. Höchste Rechenleistung ist meist überproportional teuer. Für die Datensicherung bietet sich je nach Menge der Daten ein DVD oder CD-Brenner an, da diese eine einfache Handhabung sowohl bei Sicherung als auch bei der Wiederherstellung der Daten bieten. Als Betriebssystem sollte MS Windows XP Professional eingesetzt werden, da dieses stabil läuft und auch relativ viele Programme dafür verfügbar sind. Außerdem unterstützt der OKR momentan nur MS Win XP Professional (oder ältere MS Betriebssysteme) für seine Programme. Im Gegensatz zur Home-Variante ermöglicht Professional differenziertere Sicherheitseinstellungen und ermöglicht später auch eine professionelle Vernetzung. Für die Bürokommunikation empfiehlt es sich MS Office XP oder 2003 zu nehmen, da dies einen problemlosen Austausch von Dokumenten mit vielen anderen Dienststellen ermöglicht – MS-Office ist derzeit Defacto Standard.
E-Mail	Für E-Mail-Kommunikation stehen derzeit mehrere Programme zur Verfügung. Outlook Express ist kostenlos im Betriebssystem enthalten, während Outlook meist mit dem Office-Paket geliefert wird. Alternativ gibt es noch Mozilla Thunderbird.
Virenschutz	Unbedingt notwendig ist ein Virenschutz der regelmäßig (am besten automatisch) aktualisiert wird.
Drucker: Tintenstrahldrucker; alternativ Laserdrucker Netzwerkfähiger Laserdrucker	Welche Druckerart man wählt hängt von der Art und der Menge der zu druckenden Dokumente ab. Tintenstrahldrucker sind in der Anschaffung günstig und bieten die Möglichkeit, farbige Ausdrucke zu machen. Allerdings sind die Druckkosten pro Seite relativ teuer, speziell bei Farbdrucken. Sie eignen sich somit für gelegentliche Ausdrucke mit farbigen Elementen. Laserdrucker bieten erst bei teureren Modellen Farbdrucke. Die kleineren Monochrom-Modelle eigenen sich vor allem für kleine bis mittlere Druckvolumina, die keinen Farbdruck erfordern. Die Kosten pro Seite sind deutlich geringer als bei Tintenstrahldruckern.
Printserver	Bei Peer-to-Peer vernetzen Rechnern bietet sich die Möglichkeit einen Laserdrucker mit kleinem Printserver einzusetzen. Dieser kann dann von allen angeschlossenen Rechnern genutzt werden. Meist handelt es sich dabei um einen leistungsfähigen Drucker der auch größere Ausdruck-Mengen ermöglicht.
Switch	Für die Peer-to-peer Vernetzung wird ein Switch benötigt der die einzelnen PCs verbindet. Dieser muss ausreichend Ports bieten um alle Geräte anzuschließen. Mit einzurechnen sind dabei evtl. vorhandene Netzwerkdrucker und Router. Switche sind heute mit bis zu 1 GBit/s Anschlüssen erhältlich. Allerdings reichen für den normalen Bürobetrieb Geräte mit 100 MBit/s vollständig aus.
Internet-Zugang Router mit integrierter Firewall	Um den Internetzugang für mehr als zwei PCs zu realisieren, empfiehlt es sich sowohl bei ISDN als auch bei DSL einen Router einzusetzen. Dieser baut die Internetverbindung stellvertretend für die Rechner auf und bei Nichtnutzung wieder automatisch ab. Wird der Internetzugang von mehr als einem Rechner genutzt, so teilen sich diese den Zugang über den Router automatisch. Für den Internetzugang stehen als Alternativen ISDN oder DSL zur Verfügung. ISDN ist zu empfehlen wenn nur gelegentlich Informationen aus dem Internet abgerufen werden. DSL rentiert sich bei Online-Zeiten von mehr als ca. 40 Std./Monat oder großen Download-Mengen, da hierfür sog. Flatrates verfügbar sind.

Gerät:	Bemerkung:
Funk-LAN	Funk-LANs bzw. Wireless LANs (WLANs) bieten die Möglichkeit, mit geringem Aufwand drahtlose Netze aufzubauen Aufgrund der bequemen Einrichtung der WLAN-Netze, der Übertragung auch über Grundstücksgrenzen hinaus und evtl. falsch (vor-) konfigurierter Geräte müssen mindestens folgende Datenschutz- und Sicherheitsmaßnahmen ergriffen werden: • Netzwerkname (SSID) unterdrücken • WPA-Verschlüsselung einschalten (langes Kennwort) • Zugangsfilter im Access Point einrichten (MAC-Adressen der Teilnehmer) Weitere Maßnahmen wie VPN einrichten oder DHCP deaktivieren werden empfohlen (Näheres siehe Informationsschrift "Sicherheit im Funk-LAN" des BSI, 2003).
Zugang zum OKR-Netz: Zugangskennungen IP-Adressen	Auf den Rechnern des OKR werden neben der Bürokommunikation eine Reihe weiterer Anwendungen im Bereich Personalwesen, Finanzwesen u. a. angeboten. Der Zugang erfolgt üblicherweise über das Internet und das Produkt Citrix, das auf dem lokalen PC installiert wird. Die Zugangskennung vergibt das Referat IT. Für lokale Netzwerke sollten IP-Adressen verwendet werden, die das Referat IT zuweist.

3. Dienststellen mit bis 5 und mehr PCs:

Gerät:	Bemerkung:
PC(s) mit: • Prozessor Intel/AMD mit ca. 3GHz bzw. Dual Core Prozessoren • Hauptspeicher: 512 - 1024MB • Festplatte: 80 – 250 GB • Netzwerkkarte für Peer-to-Peer-Vernetzung • Microsoft Windows XP Professional • Microsoft Office XP oder 2003	Für die normale Bürotätigkeit reicht ein PC im mittleren Preissegment aus. Höhere Rechenleistung ist nur notwendig wenn häufig aufwendige Bildbearbeitung gemacht werden soll. Höchste Rechenleistung ist meist überproportional teuer. Für die Datensicherung bietet sich je nach Menge der Daten ein DVD oder CD-Brenner an, da diese eine einfache Handhabung sowohl bei Sicherung als auch bei der Wiederherstellung der Daten bieten. Als Betriebssystem sollte MS Windows XP Professional eingesetzt werden, da dieses stabil läuft und auch relativ viele Programme dafür verfügbar sind. Außerdem unterstützt der OKR momentan nur MS Win XP Professional (oder ältere MS Betriebssysteme) für seine Programme. Im Gegensatz zur Home-Variante ermöglicht Professional differenziertere Sicherheitseinstellungen und ermöglicht später auch eine professionelle Vernetzung. Für die Bürokommunikation empfiehlt es sich MS Office XP oder 2003 zu nehmen, da dies einen problemlosen Austausch von Dokumenten mit vielen anderen Dienststellen ermöglicht – MS-Office ist derzeit Defacto Standard.
E-Mail	Für E-Mail-Kommunikation stehen derzeit mehrere Programme zur Verfügung. Outlook Express ist kostenlos im Betriebssystem enthalten, während Outlook meist mit dem Office-Paket geliefert wird. Alternativ gibt es noch Mozilla Thunderbird.
Server mit: • Prozessor Intel/AMD mit ca. 3GHz • Hauptspeicher: 1024 – 2048 MB • Festplatte(n): 160 – 400 GB (evtl. RAID) • Band-Sicherungslaufwerk • Netzwerkkarte • Microsoft Windows Server 2003 alternativ Server 2003 Small Business Edition • Sicherungsprogramm • Zentraler Virenschutz	Beim Server handelt es sich um einen weiteren Rechner im Netzwerk, der aber nicht als Arbeitsplatz genützt wird, sondern zur zentralen Datenablage dient. Außerdem werden dort die Berechtigungen für das ganze Netzwerk verwaltet und die Sicherung der Daten gemacht. Mit einem zentralen Virenschutz auf dem Server ist ein automatisches Update der PCs möglich. Wird als Betriebssystem die "Small Business Edition" gewählt kann der Server auch als zentraler Mailserver genutzt werden. Zur Erhöhung der Ausfallsicherheit kann der Server mit mehreren Festplatten ausgerüstet und diese in einem RAID-Verbund zusammengeschaltet werden. Fällt dann eine Festplatte aus, kann der Server ohne Ausfall weiter betrieben werden. Für die Sicherung der Daten ist ein Bandsicherungslaufwerk mit passendem Sicherungsprogramm notwendig. Alternativ kann auch ein DVD-Brenner verwendet werden, der aber max. 8 GB sichern kann. Wichtig sind die Kontrolle des Sicherungsprogramms und die Auslagerung der Sicherungsmedien wegen evtl. Katastrophenfällen.
Drucker: Tintenstrahldrucker; alternativ Laserdrucker Netzwerkfähiger Laserdrucker	Welche Druckerart man wählt, hängt von der Art und der Menge der zu druckenden Dokumente ab. Tintenstrahldrucker sind in der Anschaffung günstig und bieten die Möglichkeit, farbige Ausdrucke zu machen. Allerdings sind die Druckkosten pro Seite relativ teuer, speziell bei Farbdrucken. Sie eignen sich somit für gelegentliche Ausdrucke mit farbigen Elementen. Laserdrucker bieten erst bei teureren Modellen Farbdrucke. Die kleineren Monochrom-Modelle eigenen sich vor allem für kleine bis mittlere Druckvolumina, die keinen Farbdruck erfordern. Die Kosten pro Seite sind deutlich geringer als bei Tintenstrahldruckern.
Printserver	Bei Peer-to-Peer vernetzen Rechnern bietet sich die Möglichkeit einen Laserdrucker mit kleinem Printserver einzusetzen. Dieser kann dann von allen angeschlossenen Rechnern genutzt werden. Meist handelt es sich dabei um einen leistungsfähigen Drucker der auch größere Ausdruck-Mengen ermöglicht.
Switch	Für die Peer-to-peer Vernetzung wird ein Switch benötigt der die einzelnen PCs verbindet. Dieser muss ausreichend Ports bieten um alles Geräte anzuschliessen. Mit einzurechnen sind dabei evtl. vorhandene Netzwerkdrucker und Router.

Gerät:	Bemerkung:
	Switche sind heute mit bis zu 1 GBit/s Anschlüssen erhältlich. Allerdings reichen für den normalen Bürobetrieb Geräte mit 100 MBit/s vollständig aus.
Internet-Zugang Router mit integrierter Firewall	Um den Internetzugang für mehr als zwei PCs zu realisieren, empfiehlt es sich sowohl bei ISDN als auch bei DSL einen Router einzusetzen. Dieser baut die Internetverbindung stellvertretend für die Rechner auf und bei Nichtnutzung wieder automatisch ab. Wird der Internetzugang von mehr als einem Rechner genutzt, so teilen sich diese den Zugang über den Router automatisch. Für den Internetzugang stehen als Alternativen ISDN oder DSL zu Verfügung. ISDN ist zu empfehlen wenn nur gelegentlich Informationen aus dem Internet abgerufen werden. DSL rentiert sich bei Online-Zeiten von mehr als ca. 40 Std./Monat oder großen Download-Mengen, da hierfür sog. Flatrates verfügbar sind.
Funk-LAN	Funk-LANs bzw. Wireless LANs (WLANs) bieten die Möglichkeit, mit geringem Aufwand drahtlose Netze aufzubauen. Aufgrund der bequemen Einrichtung der WLANNetze, der Übertragung auch über Grundstücksgrenzen hinaus und evtl. falsch (vor-) konfigurierter Geräte müssen mindestens folgende Datenschutz- und Sicherheitsmaßnahmen ergriffen werden: • Netzwerkname (SSID) unterdrücken • WPA-Verschlüsselung einschalten (langes Kennwort) • Zugangsfilter im Access Point einrichten (MAC-Adressen der Teilnehmer) Weitere Maßnahmen wie VPN einrichten oder DHCP deaktivieren werden empfohlen (Näheres siehe Informationsschrift "Sicherheit im Funk-LAN" des BSI, 2003).
Zugang zum OKR-Netz: Zugangskennungen IP-Adressen	Auf den Rechnern des OKR werden neben der Bürokommunikation eine Reihe weiterer Anwendungen im Bereich Personalwesen, Finanzwesen u. a. angeboten. Der Zugang erfolgt üblicherweise über das Internet und das Produkt Citrix, das auf dem lokalen PC installiert wird. Die Zugangskennung vergibt das Referat IT. Für lokale Netzwerke sollten IP-Adressen verwendet werden, die das Referat IT zuweist.

Anlage 2: Software für externe Dienststellen

Diese Anlage enthält Empfehlungen zum Softwareeinsatz für kleine und mittlere Einrichtungen (in Ergänzung zum IT-Konzept und in Ergänzung zu der in Analage 1 beschriebenen Hardware-Ausstattung).

Auch hier wird zunächst der für den geordneten Ablauf in einer Dienststelle benötigte Softwarebedarf beschrieben, darüber hinaus werden aber auch Empfehlungen für Programme ausgesprochen, die in kleineren und mittleren Dienststellen von der gegenüber großen Einrichtungen anderen Aufgabenstellung her benötigt werden (z. B. Gemeindebaukasten). Außerdem sind hier in Ergänzung zu den Ausführungen in Kapitel XI Datenschutz und Datensicherheit die als Freeware oder Shareware erhältlichen Programme zur Unterstützung der täglichen Arbeit aufgeführt.

Anmerkung: Windows Vista und Office 2007 sind neue Softwareprodukte der Firma Microsoft. Gegenwärtig unterstützt Windows Vista noch nicht alle Anwendungsprogramme unserer Landeskirche (z. B. Kifikos). Insbesondere im Modul Powerpoint und im Makrobereich sollte zurzeit mit Kompatibilitätsproblemen gerechnet werden, die sich durch spezielle Tools von MS nicht vollständig beseitigen lassen. Aus diesen Gründen wird gegenwärtig nicht empfohlen Windows Vista und Office 2007 umgehend einzusetzen. Es wird an dieser Stelle ausdrücklich darauf hingewiesen, dass es sich hierbei um eine vorläufige Empfehlung handelt.

1. Betriebssysteme

Software	Kurzbeschreibung	Beschreibung/ Voraussetzungen
Windows Vista	Anfang des Jahres 2007 neu auf den Markt gekommen. Von einem sofortigen Einsatz wird dringend abgeraten, da die erforderlichen Gerätetreiber noch nicht in vollem Umfang zur Verfügung stehen und eine Reihe von Anwenderprogrammen auf dieses neue Betriebssystem noch nicht angepasst sind.	Kommerzielle Software Systemvoraussetzung: Pentium IV bzw. Dual Core Prozessoren oder vergleichbare Prozessoren von AMD Speicher 1024 MB RAM
Windows XP Pro	Zurzeit Standard bei neuen PCs. Falls bei Auslieferung nur WIN XP home enthalten ist, wird die Aufrüstung auf WIN XP Pro empfohlen.	Kommerzielle Software Systemvoraussetzung: Pentium III oder höher bzw. vergleichbare Prozessoren von AMD Speicher mind. 256 MB RAM empf. 512 MB RAM
Windows 2000	Standard für vorhandene Personalcomputer	Kommerzielle Software Systemvoraussetzung: Pentium III oder höher bzw. vergleichbare Prozessoren von AMD Speicher mind. 128 MB RAM empf. 256 MB RAM

2. Office-Anwendungen

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
MS Office 2007	Anfang des Jahres 2007 neu auf den Markt gekommen. Von einem sofortigen Einsatz wird abgeraten, da mit größeren Umstellungsarbeiten vor der Benutzung des Programms gerechnet werden muss. Dies gilt sowohl für einen erhöhten Schulungsbedarf, weil die Benutzung der Software vom Hersteller angepasst wurde als auch bei der Kommunikation mit den Vorgängerversionen.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP/VISTA
MS Office 97 bis 2003	Standardmäßig verwendetes Officesystem. Ab Office 2003 werden Windows 2000 oder XP vorausgesetzt.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP/Vista
OpenOffice	Leistungsfähiges Officepaket. Der Einsatz ist bisher nicht erprobt. Die Übernahme von Dateien zwischen Microsoft Office und Open Office erfolgt nicht immer fehlerfrei.	Open Source Systemvoraussetzung: WIN 98SE/2000/XP/Vista/LINUX

3. Web Browser

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
MS Internet Explorer	Weit verbreiteter Internetbrowser. Weiterentwicklung nur noch für WIN 2000 und XP	Freeware Systemvoraussetzung: WIN 2000/XP/Vista
Mozilla Firefox	Alternative zum Internet Explorer.	Open Source Systemvoraussetzung: WIN 98SE/2000/XP/Vista/LINUX
Opera	Alternative zum Internet Explorer.	Freeware Systemvoraussetzung: WIN 2000/XP

4. Mail Server

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
Microsoft Exchange	Server für die zentrale Verwaltung von Mails, Terminen und Kontakten. Setzt einen Server voraus; auch als Paket Microsoft Small Business Server erhältlich.	Kommerzielle Software Systemvoraussetzung: WIN 2000/2003 Server
AVM KEN!3	Einfacher Mail-, Proxy und CAPI-Server für kleinere Netzwerke	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP/2003
JanaServer	Einfacher Mail- und Proxy-Server für kleinere Netzwerke	Kostenlos für nichtkommerziellen Einsatz Systemvoraussetzung: WIN 98SE/2000/XP

5. Firewall, Virenscanner, Antispyware

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
Symantec Norton Internet Security	Firewall und Virenscanner (auch als reiner Virenscanner erhältlich: Norton AntiVirus)	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
Mcafee Internet SecuritySuite	Firewall und Virenscanner (auch als reiner Virenscanner erhältlich: virusscan)	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP
H+BEDV AntiVir PersonalEdition Classic	Virenscanner	Freeware Systemvoraussetzung: WIN 98SE/2000/XP
ZoneAlarm	Firewall; bietet erweiterte Möglichkeiten gegenüber der Windows XP-Firewall	Kostenlos für nichtkommerziellen Einsatz Systemvoraussetzung: WIN 98SE/2000/XP
Windows XP-Firewall	Firewall. Diese einfache Firewall ist bereits kostenlos im Betriebsystem enthalten.	kostenlos Systemvoraussetzung: WIN XP
Ad-Aware Personal	Software zum Auffinden und löschen von unerwünschten Programmen (Spyware).	Kostenlos für nichtkommerziellen Einsatz Systemvoraussetzung: WIN 98SE/2000/XP
Search & Destroy	Software zum Auffinden und löschen von unerwünschten Programmen (Spyware).	Freeware Systemvoraussetzung: WIN 98SE/2000/XP

6. Anwenderprogramme

6.1. Bildbearbeitung

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
IrfanView	Einfaches und übersichtliches Bildbearbeitungsprogramm mit Batchkonvertierung aber eingeschränktem Funktionsumfang	Freeware Systemvoraussetzung: WIN 98SE/2000/XP
Gimp	Leistungsfähiges aber nicht besonders übersichtliches Bildbearbeitungsprogramm.	Open Source Systemvoraussetzung: WIN 98SE/2000/XP/LINUX
Photoshop	Leitungsfähiges und weit verbreitetes Bildbearbeitungsprogramm.	Kommerzielle Software Systemvoraussetzung: WIN 2000/XP/Vista

6.2. Präsentation und Projektarbeit

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
MS PowerPoint	Weit verbreitetes Standardprogramm für Präsentationen mit Beamer.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP/Vista
Impress (OpenOffice)	Äquivalent zu MS Powerpoint. Der Einsatz ist bisher nicht erprobt. Die Übernahme von Dateien zwischen Microsoft Powerpoint	Open Source Systemvoraussetzung:

Standard	Beschreibung/Definition	Beschreibung/ Voraussetzungen
	und Impress erfolgt nicht immer fehlerfrei.	WIN 98SE/2000/XP/Vista/LINUX
Mind Manager oder Openmind	Einfach zu handhabende Programme zur übersichtlichen Darstellung von Zusammenhängen.	Kommerzielle Software Systemvoraussezung: WIN 98SE/2000/XP
MS Project	Werkzeug zur Planung und Kontrolle umfangreicher und komplexer Projekte.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP/Vista
GanttProject	Werkzeug zur Planung und Kontrolle mittlerer und komplexer Projekte.	Open Source Systemvoraussetzung: WIN 98SE/2000/XP/LINUX

6.3. Personalwesen

Standard	Beschreibung**/Definition**	Beschreibung**/** Voraussetzungen
pcBAT TVöD	Als Ergänzung der Software im Bereich Personalwesen empfohlen.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP
Gehaltsrechner: gehalt.de	Als Ergänzung der Software im Bereich Personalwesen einsetzbar.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP
Lexware lohn + gehalt	Als Ergänzung der Software im Bereich Personalwesen einsetzbar.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP
Haufe TVöD - Office	Informationssystem für die BAT-Personalarbeit	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP
Haufe– Personal Office	Informationssoftware für den Personalbereich	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP
SV.Net	Erstellung und Übermittlung von Sozialversicherungsmeldungen und Beitragsnachweise an die Krankenkassen.	kostenlos Systemvoraussetzung: WIN 98SE/2000/XP

7. Utilities

7.1. Packprogramme

Software	Kurzbescheibung	Beschreibung/ Voraussetzungen
WinZip	Komfortables und weit verbreitetes Programm zum Packen und Entpacken von Dateien bzw. Verzeichnissen.	Shareware Systemvoraussetzung: WIN 98SE/2000/XP
Power Archiver 2000	wie oben	Freeware Systemvoraussetzung: WIN 98SE/2000/XP
Power Archiver 2007	wie oben	Shareware Systemvoraussetzung: WIN 98SE/2000/XP/VISTA

7.2. Backup

Software	Kurzbescheibung	Beschreibung/ Voraussetzungen
Veritas Backup Exec	Software zur automatisierten Sicherung von Servern und deren Diensten	Kommerzielle Software Systemvoraussetzung: WIN 2000/2003
Windows Sicherungsprogramm	Software zur Sicherung von Daten auf Einzelplatz-Rechner und Server	Kostenlos im Betriebssystem enthalten Systemvoraussetzung: WIN 2000/XP/2003
Backup Slave	Backup auch auf externe Laufwerke (auch Sticks) und Brenner möglich.	Freeware Systemvoraussetzung: WIN 98SE/2000/XP

7.3. Brennsoftware

Software	Kurzbescheibung	Beschreibung/ Voraussetzungen
Nero	Einfach zu bedienendes Programm zum Brennen von CDs und DVDs.	Kommerzielle Software Systemvoraussetzung: WIN 98SE/2000/XP/VISTA/LINUX
Burn4Free	Einfaches Brennprogramm für CDs und DVDs.	Freeware Systemvoraussetzung: WIN 98SE/2000/XP

7.4. Viewer

Software	Kurzbescheibung	Beschreibung/ Voraussetzungen
Adobe Reader	Programm zum Anzeigen und Drucken von PDF-Dateien sowie zum Suchen in diesen Dateien.	Freeware Systemvoraussetzung: WIN 98SE/2000/XP/VISTA/LINUX

7.5. PDF-Konverter

Software	Kurzbescheibung	Beschreibung/ Voraussetzungen
FreePDF XP	Umwandlung beliebiger Anzeigeformate in PDF-Dateien(auch Word, Excel, usw.). Zusammenfügen mehrerer PDF-Dateien zu einer Datei.	Freeware Systemvoraussetzung: WIN 2000/XP

7.6. HTML-Editor

Software	Kurzbescheibung	Beschreibung/ Voraussetzungen
Gemeindebaukasten	Einfach zu handhabender Softwarebaukasten zum Erstellen von Internetseiten.	Software vom Evangelischen Medienhaus Stuttgart zusammengestellt Systemvoraussetzung: WIN 98SE/2000/XP

Anlage 3: Preisliste für Leistungen im Referat Informationstechnologie

-Stand November 2012-

Leistung	EURO	
	einmalig	lfd.
Full - Service Basisdienste / Betreuung Standard Arbeitsplatz OKR: (Monatspauschale pro E-Mail Postfach) Systemzugang, Systemaktualität, Software-Paketierung (Standard SW), automatisierte Softwareverteilung, Datensicherung, Systemsicherheit inkl. Viren- & Spamschutz, Homeshare, Gruppenshare, Infosystem, Telefon-Support, Helpdesksystem, Infrastruktur OKR, Netzwerkmanagement		130,00
Betreuung angeschlossene externe Dienststellen (OKR Server) (Monatspauschale / E-Mail Postfach) Systemzugang, Systemaktualität, Software-Paketierung (Standard SW), automatisierte Softwareverteilung, Datensicherung, Systemsicherheit inkl. Viren- & Spamschutz, Telefon-Support Helpdesksystem, Infrastruktur OKR, Netzwerkmanagement		70,00
Betreuung Dienststellen mit eigenen Server (Monatspauschale / E-Mail Postfach) Bereitstellung eines redundanten Internetzugangs über die Systemumgebung des OKR, Zentraler Virenschutz für einkommende E-Mails, Spamfilter für einkommende E-Mails, Kontaktintegration in Outlook, Empfang / Versand / Weiterleitung E-Mails an die Dienststelle, Telefon-Support.		13,00

Anlage 4: Abkürzungsverzeichnis

Abkürzung	Bedeutung
AD	Active Directory
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
ASP	Active Server Page oder Application Service Providing
ATM	Asynchronous Transfer Mode
BK	Bürokommunikation
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAD	Computer Aided Design
CASE	Computer Aided Software Engineering
CD ROM	Compact Disk Read only Memory
CERT	Computer Emergency Response Team
CE	Communauté Européenne
COM	Component Object Model
CORBA	Common Object Request Broker Architecture
COS	Common Object Services
C/S	Client-Server
DB	Datenbanken
DBMS	Datenbank Management System
DCOM	Distributed Component Object Modell
DDE	Dynamic Data Exchange
DDL	Data Definiton Language
DES	Data Encryption Standard
DML	Data Manipulation Language
DNS	Domain Name Service
DSA	Directory Service Agent oder Digital Signature Algorithmus
DSS 1	Digital Subscriber Signaling System No.1
DTD	Document Type Definition
DV	Datenverarbeitung
DVD	Digital Versatile Disc
DXF	Drawing Exchange Format
ECC	Elliptic Curve Cryptography
ECMA	Verband der europäischen Computerhersteller (European Computer Manufacturers Association)
EDS	Electronic Data Systems
e-GK	e-Government-Konzept (vormals Landessystemkonzept des Landes Baden-Württemberg)
EJB	Enterprise Java Beans
EMV	Elektromagnetische Verträglichkeit von Geräten
EMVG	Gesetz über die elektromagnetische Verträglichkeit von Geräten

Abkürzung	Bedeutung
WPA	Wireless Protected Access (Verschlüsselungsprotokoll bei Funk-LAN)
WWW	World Wide Web
XML	Extensible Markup Language
XP	Experience (neuestes Windows-Betriebssystem für Clients)
XSL	Extensible Stylesheet Language