Intranet der EKHN

Häufig gestellte Fragen (FAQ)

Stand: 16.11.2006

Neuauflage!

Erstellt von:

Ev. Regionalverwaltung
Wiesbaden-Rheingau-Taunus

Steffen Grellmann

In diesem Dokument verwendete Symbole

	Nützlicher Hinweis.
	Wichtiger Hinweis. Nichtbeachtung kann zu einem Fehlverhalten des Systems führen.
	Bitte prüfen Sie, ob die beschriebenen Voraussetzungen gegeben sind.
	Begriffserklärung.
	Ansprechpartner in Kurzform. Die vollständigen Anschriften befinden sich im Anhang, Kapitel. 6.1.

Impressum

Ev. Regionalverwaltung Wiesbaden-Rheingau-Taunus

EDV-Koordination
Steffen Grellmann
Schwalbacher Str. 6
65185 Wiesbaden
Telefon: 0611-1409-231
Telefax: 0611-1409-273
E-Mail: Steffen.Grellmann@ekhn-kv.de

In dieser Broschüre erfahren Sie alles, was Sie über das Intranet der EKHN und den EDV-Einsatz in den Dienststellen der EKHN wissen müssen.

Inhalt

1. Über diese Broschüre

Den Gemeinden, Dienststellen und Einrichtungen der EKHN steht seit 2002 ein Intranet zur Verfügung. Dieses Intranet erleichtert die dienstliche Kommunikation, stellt der internen Öffentlichkeit Informationen und Arbeitshilfen zur Verfügung und bildet die Grundlage für den Zugriff auf kirchliche Programme und Datenbanken, beispielsweise die Gemeindegliederverwaltung mit netKIM.

In dieser Broschüre finden Sie wichtige Informationen zum Intranet und zum Einsatz elektronischer Datenverarbeitung im Allgemeinen. Auf die erforderlichen Voraussetzungen, mögliche Fehlerquellen bei der Installation und die technischen Hintergründe wird detailliert eingegangen und es werden wertvolle Hinweise zum Beheben technischer Probleme gegeben. Darüber hinaus sind in dieser Broschüre die einzelnen, über das Intranet zugänglichen kirchlichen Programme kurz beschrieben und weiterführende Ansprechpartner benannt.

FAQ

FAQ ist die Abkürzung für „*Frequently Asked Questions*“, zu deutsch „Häufig gestellte Fragen“.

Diese FAQ-Broschüre erhebt nicht den Anspruch, detaillierte Anleitungen zur Hand zu geben. Vielmehr wurde versucht, möglichst alle Aspekte des Intranets in einem Dokument zusammenzufassen und Hilfestellung bei Fragen oder Problemen zu geben. Die technischen Zusatzinformationen richten sich insbesondere auch an das Fachpublikum, das mit der EDV-Betreuung in den Dienststellen vor Ort betraut ist.

2.1 Was ist ein Intranet?

Ein Intranet ist ein geschützter Bereich innerhalb des öffentlichen Internets. Durch die Abschirmung gegenüber dem öffentlichen Netz eignet es sich hervorragend für den Austausch interner Daten.

2.2 Wozu wird in der EKHN ein Intranet benötigt?

Informationsplattform

Der Intranet-Zugang ermöglicht den Zugang zu den internen Webseiten der EKHN („Informationsplattform“) mit dem Anschriftenverzeichnis, der Rechtssammlung, einem Downloadbereich für Vordrucke und Arbeitshilfen und vielem anderen mehr. Einzelne Regionalverwaltungen, wie auch die Ev. Regionalverwaltung Wiesbaden-Rheingau-Taunus, sind auf der Informationsplattform mit eigenen Bereichen vertreten (Aufruf über: Kirche vor Ort > Reg.-Verwaltungen).

Kirchliche Programme im Intranet

Darüber hinaus bildet der Intranet-Zugang die Grundlage für die Nutzung kirchlicher Programme wie **netKIM**, der **KFM-Webauskunft** für das Finanzwesen oder **WinKita on Web**. Da es sich hier um Web-basierte Programme handelt, auf die mit Hilfe des Webbrowsers zugegriffen wird, muss keine zusätzliche Software installiert werden.

E-Mail

Jede kirchliche Einrichtung bzw. jede(r) Intranet-Benutzer(in) erhält im Rahmen des Intranet-Zugangs eine dienstliche E-Mail-Adresse mit der Endung „@ekhn-net.de“. Nach der neuen, für die EKHN gültigen IT-Verordnung (Amtsblatt Nr. 4/2006 vom 01.01.2006, S. 118 f) muss dienstliche Kommunikation, sofern diese per E-Mail erfolgt, ausschließlich über

dienstliche E-Mail-Adressen geführt werden.

2.3 Welche Rechtsgrundlagen sind für das Intranet maßgebend?

Die Einführung des Intranets sowie das Investitionsprogramm gehen auf einen Beschluss der EKHN-Synode zurück.

Der Einsatz von Informationstechnologie wird durch die „Verwaltungsverordnung über den Einsatz von Informationstechnologie“ (IT-Verordnung - ITVO) vom 01.04.2006 geregelt. Daneben sind die Sicherheitsrichtlinie und die Regelung zum Passwortgebrauch zu beachten, die ergänzend zur IT-Verordnung erlassen wurden. Die IT-Verordnung, die Sicherheitsrichtlinie und die Regelung zum Passwortgebrauch gelten für alle Einrichtungen der EKHN.

Die Dienstvereinbarung zwischen Dekanat und MAV regelt Einführung und Nutzung von Internet, Intranet und E-Mail.

Für die Anmeldung zum Intranet ist die Zustimmung von Kirchenvorstand bzw. Dienststellenleitung erforderlich.

2.4 Wer ist für das Intranet verantwortlich?

Für das Gesamtprojekt verantwortlich ist das Fachreferat Informationstechnologie der Kirchenverwaltung, für die Informationsplattform das Referat Öffentlichkeitsarbeit. Für die Betreuung der kirchlichen Programme im Internet gibt es im Fachreferat Informationstechnologie bei der Kirchenverwaltung jeweils eine(n) Fachreferentin bzw. -referenten als Ansprechpartner(in).

Anschriften siehe Anhang.

2.5 Wie wird die Datensicherheit gewährleistet?

VPN

VPN ist die Abkürzung für „*Virtuelles privates Netzwerk*“. Beim *VPN* wird über das öffentliche Internet ein gesicherter und verschlüsselter Datentunnel zwischen Ihrem PC und der Kirchenverwaltung bzw. dem Rechenzentrum aufgebaut.

Technische Absicherung

Das Intranet ist ein virtuelles Netzwerk (VPN) innerhalb des öffentlichen Internets. Da über die gleichen Leitungen der öffentliche Internetverkehr erfolgt, muss das Intranet gegenüber der Öffentlichkeit besonders gut abgeschirmt werden. Diese Abschirmung wird durch den Einsatz von VPN und einer zentralen Firewall gewährleistet.

Zugang zum Intranet ist nur den Personen und Einrichtungen möglich, die sich schriftlich zur Teilnahme am Intranet bei der Kirchenverwaltung angemeldet haben und die über eine Nutzerkennung, ein Kennwort und eine Schlüsseldatei verfügen.

Rechtliche Rahmenbedingungen

Mit der Anmeldung zum Intranet wird die Sicherheitsrichtlinie der EKHN (Anlage zur IT-Verordnung) akzeptiert.

Über die technischen Maßnahmen hinaus sind zur Gewährleistung der Datensicherheit folgende Verordnungen und Richtlinien maßgebend:

- „Verwaltungsverordnung über den Einsatz von Informationstechnologie“ (IT-Verordnung - ITVO) vom 01.04.2006
- Regelung zum Passwortgebrauch
- Sicherheitsrichtlinie der EKHN

Eine Zusammenfassung der wichtigsten Regelungen finden Sie auf http://www.ekhn.de:

Datenschutz und Datensicherheit
http://www.ekhn.de/intranet/download/sicherheit_datenschutz.pdf

Datenschutzbeauftragter

Die evangelischen Landeskirchen Hessen-Nassau und Kurhessen-Waldeck verfügen über einen gemeinsamen Datenschutzbeauftragten. Zu seinen Aufgaben gehört es, die Einhaltung von Datenschutz und Datensicherheit in den Einrichtungen der beiden Landeskirchen zu überwachen und Empfehlungen zu deren Verbesserung zu entwickeln. Für die Dienststellen und Kirchenmitglieder steht der Datenschutzbeauftragte bei Fragen beratend zur Verfügung.

Ansprechpartner: Kirchenverwaltung

2.6 Wer kann sich für die Teilnahme am Intranet anmelden?

Anmelden können sich Kirchengemeinden, Kindertagesstätten, Diakoniestationen, Dekanatsgeschäftsstellen, Pfarrerinnen und Pfarrer sowie die haupt-, neben- und ehrenamtlich Mitarbeitenden. Die Zustimmung von Kirchenvorstand bzw. Dienststellenleitung ist erforderlich.

2.7 Wie erhält man Anschluss an das Intranet?

Stellen Sie sicher, dass Sie über einen funktionsfähigen Zugang zum Internet verfügen und das Ihr PC möglichst wie in Kapitel 3.5 beschrieben konfiguriert ist.

1. Melden Sie sich bei der Kirchenverwaltung der EKHN für die Teilnahme am Intranet an. Anmeldeformulare finden Sie auf http://www.ekhn.de:

   klicken Sie hier entweder auf **> Intranet für Mitarbeitende der EKHN** oder auf **A-Z > Intranet**.

2. Anschließend erhalten Sie von der Kirchenverwaltung die Installations-CD, eine gedruckte Anleitung sowie Ihre Zugangskennung per Post zugeschickt.

3. Nachdem Sie von der CD die Intranet-Software (diese besteht aus VPN-Client, Firewall- und Antivirenprogramm) installiert haben, sind alle Voraussetzungen für die Nutzung des Intranets erfüllt.

2.8 Welcher Internetprovider und –tarif ist empfehlenswert?

Wir empfehlen einen T-DSL-Business-Anschluss in Verbindung mit einer Flatrate. Im Vergleich mit dem T-DSL-Anschluss für Privatkunden bietet die Business-Variante eine Reihe von Vorteilen, z.B. einen festen Ansprechpartner beim Großkundenservice der Telekom (über Regionalverwaltung) und eine spezielle kostenfreie Hotline bei Problemen mit den Zugangsdaten

Eine eigene Domain (www.meine-firma.de) ist Bestandteil des Zugangs.

Der monatliche Grundpreis für eine Flatrate in Verbindung mit T-DSL-Business beträgt nur noch 5,90 €. Von den minutengenauen Abrechnungstarifen hingegen ist dringend abzuraten, da diese ein unkalkulierbares Kostenrisiko bedeuten.

Mittlerweile sind DSL-Anschlüsse zu vertretbaren Kosten bis 6.016 kbit/s

DSL

(Digital Subscriber Line) ist eine Breitband-Technologie, die über die herkömmliche Telefonleitung hohe Übertragungsraten und einen sehr schnellen Seitenaufbau im Internet ermöglicht. PC und Telefon können gleichzeitig verwendet werden.

Flatrate

Bei einer *Flatrate* zahlt man einen monatlichen Pauschalbetrag und kann dafür so lange

online sein wie man möchte.

verfügbar. Für den Einstieg bzw. für die Anbindung eines einzelnen Computers an Internet und Intranet dürften ein T-DSL-Business 1000-Zugang (Übertragungsrate Downstream 1.024 kbit/s) – zumindest für den Einstieg - ausreichend sein. Für die Anbindung mehrerer Computer mit Hilfe der Gateway-Lösung für kleine Netzwerke wird zu einer höheren Bandbreite (z.B. T-DSL-Business 2000 oder 6000) geraten.

In Gegenden ohne DSL-Abdeckung, z.B. im ländlichen Raum, können UMTS oder Internet via Kabel-TV eine mögliche Alternative sein. Im Gegensatz zu ISDN stehen für diese Technologien pauschalierte Flatrate-Tarife zur Verfügung, die nicht die Kostenrisiken einer minutengenauen Abrechnung beinhalten.

UMTS

(Universal Mobile Telecommunication System) ist das Mobilfunksystem der sogenannten "dritten Generation", das aufgrund hoher Übertragungsraten neben Sprachkommunikation auch Multimedia- und Internet-Anwendungen erlaubt. *UMTS* ermöglicht Übertragungsraten bis 384 kbit/s.

2.9 Wie beantrage ich einen Internetanschluss für unsere Einrichtung?

Aus organisatorischen Gründen sollen im Zuständigkeitsbereich der Regionalverwaltung Wiesbaden-Rheingau-Taunus alle Telekom-Angelegenheiten zentral über die Regionalverwaltung abgewickelt werden.

Ihre Aufträge für Telefon- und DSL-Anschlüsse, Tarifänderungen und dergleichen senden Sie bitte zusammen mit einer Kopie des Vorstandsbeschlusses direkt an die Ev. Regionalverwaltung Wiesbaden–Rheingau-Taunus (z.Hd. Herrn Otto). Anderenfalls kann nicht garantiert werden, dass eine korrekte Zuordnung der von Ihnen beantragten Leistungen zu Ihrer Einrichtung erfolgt und das ggf. bestellte Endgeräte an die richtige Lieferanschrift adressiert werden.

Ansprechpartner: Regionalverwaltung

Gateway

Ein *Gateway* ist ein Gerät, das unterschiedliche Rechnernetze miteinander verbindet.

2.10 Welche Empfehlung gibt es für die Anbindung mehrerer Computer (kleine Netzwerke) an das Intranet?

Der Intranet-Zugang ist in zwei Varianten verfügbar: Als Software-Lösung für die Installation auf Einzelplatzcomputern und als Gateway-Lösung für die Anbindung dienstlicher Netzwerke an das Intranet. Die Unterschiede dieser beiden Varianten werden in Kapitel 3.1 beschrieben.

Weiterführende Information zu der Netzwerklösung finden Sie im Internet:

Intranet-Konzept
http://www.ekhn.de/intranet/

Informationen zur Netzwerklösung
http://www.ekhn.de/intranet/download/netzwerke_info.pdf

Fragebogen
http://www.ekhn.de/intranet/download/fragenkatalog_vpn_v22.pdf

Auftrag "Kleine Netzwerklösung"
http://www.ekhn.de/intranet/download/auftrag_kleine_netzwerkloesung.doc

Ansprechpartner: Kirchenverwaltung

2.11 Welche Zuschüsse gibt es bzw. gab es?

Achtung: Betrifft nur die Einrichtungen, die den Zuschuss noch nicht erhalten haben.

Dekanatsbeauftragte

Diese Funktion wird meist von Ehrenamtlichen oder von Pfarrer(innen) als Zusatzauftrag wahrgenommen. Aufgabe der *Dekanatsbeauftragten* ist die Einführung des Intranets in den Dienststellen der EKHN zu koordinieren und das Zuschussverfahren zu überwachen.

Alle Kirchengemeinden und Kindertagesstätten hatten Anspruch auf einen einmaligen Förderbetrag zur Anschaffung eines Computers nebst Software und Zubehör sowie für die Schulung der Anwender(innen). Für die Zuteilung der Förderbeträge sind die Dekanate zuständig. Für die an das Dekanat Wiesbaden angeschlossenen Einrichtungen beläuft sich der Förderbetrag auf 2.045 €. Dieser Förderbetrag kann von Dekanat zu Dekanat differieren.

Sollten Sie zu den wenigen Einrichtungen gehören, die den Zuschuss noch nicht erhalten haben, setzen Sie sich umgehend mit der für Sie zuständigen Dekanatsgeschäftsstelle oder mit dem Dekanatsbeauftragten für das Investitionsprogramm in Verbindung. Die Anschriften finden Sie im Kapitel 6.1 „An welche Ansprechpartner kann ich mich wenden?“.

2.12 Wo gibt es Antragsformulare für die Anmeldung zur Teil nahme am Intranet?

Einzelplatz-Zugang

Formular zur Einzelanmeldung zum Ausfüllen am PC
http://www.ekhn.de/intranet/download/anmeldung_intranet_einzel.pdf

Router

Ein *Router* ist ein Gerät, das Datenpakete von einem Netzwerk in ein anderes weiterleitet. Mit einem *Router* kann auf allen Computern eines lokalen Netzwerks der Zugang zum Internet ermöglicht werden.

Änderung der Zugangsart zum Intranet: Formular für Einzelanwender / innen mit DSL-Router
http://www.ekhn.de/intranet/download/anmeldung_intranet_einzel_dsl.pdf

Netzwerklösung

Informationen
http://www.ekhn.de/intranet/download/netzwerke_info.pdf

Fragebogen
http://www.ekhn.de/intranet/download/fragenkatalog_vpn_v22.pdf

Auftrag "Kleine Netzwerklösung"
http://www.ekhn.de/intranet/download/auftrag_kleine_netzwerkloesung.doc

2.13 Welche Schulungsveranstaltungen werden angeboten?

Regionalverwaltung

Die Ev. Regionalverwaltung Wiesbaden-Rheingau-Taunus hat in den letzten Jahren eine Vielzahl an Schulungen zu den Themen Intranet, netKIM, KFM-Webauskunft und zur Inventarverwaltung angeboten, organisiert und durchgeführt. Weitere Schulungsangebote werden folgen; für 2007 sind vorrangig Schulungen zu „Winkita On Web“ geplant.

Kirchenverwaltung

Darüber hinaus können die Fortbildungsangebote der Kirchenverwaltung genutzt werden. Nähere Informationen zu Themen und Terminen finden Sie im Intranet und in der Broschüre „Wissenswerte“.

Externe Anbieter

Zur Schulung allgemein gebräuchlicher Programme wie Windows, Word, Excel, Outlook, Internet-Explorer, Powerpoint und Bildbearbeitung wird auf externe Anbieter wie VHS, Volksbildungswerk, Hess. Verwaltungsschulverband usw. verwiesen.

Ansprechpartner: Regionalverwaltung

2.14 Wo gibt es weiterführende, schriftliche Informationen?

Alles Wissenswerte auf einen Blick
http://www.ekhn.de/intranet/download/info_allg.pdf

Informationen zur Gateway-/Netzwerklösung
http://www.ekhn.de/intranet/download/netzwerke_info.pdf

und auf http://www.ekhn.de: klicken Sie hier entweder auf **> Intranet für Mitarbeitende der EKHN** oder auf **A-Z > Intranet**.

Diese FAQ-Broschüre
http://www.ekhn.de/intranet/download/faqs.pdf

Eine gedruckte Anleitung in der die Installation des Intranet-Zugangs ausführlich beschrieben ist, erhalten Sie zusammen mit der Intranet-CD von der Kirchenverwaltung.

2.15 Besteht ein kirchlicher Rahmenvertrag für Microsoft-Produkte?

Die Kirchenverwaltung der EKHN hat zu diesem Thema am 25.01.2005 die folgende Information im Intranet veröffentlicht:

Günstige Konditionen für Microsoft-Produkte

Gemeinden und Einrichtungen in der EKHN können über die KIGST (Kirchliche Gemeinschaftsstelle für Elektronische Datenverarbeitung) wesentlich günstiger Microsoftprodukte einkaufen. Über den Rahmenvertrag „KIGST Select Academic“ erhalten die folgenden Einrichtungen gegenüber dem Listenpreis um bis zu 75 % ermäßigte Einkaufspreise: Gemeinden, Dekanate, Beratungsstellen, PfarrerInnen im Schuldienst, Bildungswerke und Bildungsstätten, Sonderseelsorgeeinrichtungen, Büchereien, Krankenhäuser, Diakoniestationen, Altenpflegeeinrichtung, Gustav-Adolf-Werk und Martin-Lutherbund sowie die Regionalverwaltungen.

Zusätzliche Hinweise

Die ermäßigten Einkaufspreise für Microsoft-Produkte gelten ausschließlich für dienstlich angeschaffte und genutzte Software. Privatpersonen oder Ehrenamtliche sind von der Rahmenvereinbarung ausgenommen.

Bei der KIGST erworbene Softwareprodukte bestehen aus einer Lizenz, mit der man das Recht die Software im Rahmen der Lizenzbestimmungen zu benutzen, erwirbt, und einem Installationsdatenträger (CD), der separat erworben werden muss. Bei Bestellungen unterhalb 300 € netto kommt eine Bearbeitungsgebühr hinzu. Trotzdem ist bei der KIGST über den Rahmenvertrag gekaufte Software in der Regel immer noch günstiger als wenn man die Software im normalen Handel kaufen würde.

KIGST, E-Mail: pcsc@kigst.de

2.16 Welche Empfehlung gibt es zum Thema Internet-Telefonie (VoIP)?

Voice-Over-IP

Voice-Over-IP ermöglicht das kostengünstige Telefonieren über das Internet. Bei *Voice-Over-IP* wird das Sprachsignal in Datenpakete umgesetzt und über das Internet Protokoll (IP) gesendet.

Die Internet-Telefonie (Voice-Over-IP) findet als Alternative zu den klassischen Telefonie-Diensten zunehmende Verbreitung im Massenmarkt.

Auf Grund der Sicherheitsproblematik bei der Internet-Telefonie und um die absolute Vertraulichkeit von Gesprächen im seelsorgerlichen Bereich zu

gewährleisten, wird vom dienstlichen Einsatz von Internet-Telefonie abgeraten. Die möglichen Einsparungen stehen nicht im Verhältnis zu den Risiken. Zudem scheint der Kostenvorteil von Voice-Over-IP vor dem Hintergrund zunehmend verfügbarer Telefonie-Flatrates fraglich.

Die Kirchenverwaltung hat die Fa. NorCom (Anbieter von Sicherheitslösungen für den IT-Bereich) vor einiger Zeit mit einer schriftlichen Ausarbeitung zu diesem Thema beauftragt, die bei Herrn Grellmann angefordert werden kann.

Ansprechpartner: Regionalverwaltung

WLAN

ist die Abkürzung für *Wireless Local Area Network* und bezeichnet ein Netzwerk, das nicht auf Kabel als Verbindungselemente angewiesen ist, da die Datenübermittlung per Funk erfolgt.

2.17 Welche Empfehlung gibt es für den dienstlichen Einsatz von Funknetzwerken (WLAN)?

In manchen Dienststellen kommen neben kabelgebundenen, lokalen Netzwerken (LAN) in zunehmendem Umfang auch drahtlose Netzwerke (WLAN) zum Einsatz. Der Einsatz von WLAN-Technologie in dienstlichen Netzwerken ist nicht generell unzulässig. Da die Reichweite drahtloser Netzwerke aber nicht unbedingt auf die Gebäudegrenzen beschränkt ist und es Dritten mit relativ einfachen Mitteln teilweise leicht möglich ist, von außen auf Netzwerkressourcen zuzugreifen, müssen dienstlich genutzte Funknetzwerke so sicher wie nach derzeitigem Stand der Technik möglich konfiguriert werden.

LAN

ist die Abkürzung für *Local Area Network. Als LAN* bezeichnet man ein räumlich begrenztes Netzwerk von Computern, meist innerhalb eines Unternehmens oder einer Behörde. Durch so verbundene Computer können Ressourcen wie Internetzugang, Drucker und Software gemeinsam genutzt werden.

Hierzu sind folgende Maßnahmen erforderlich:

- Verschlüsselung mittels WPA wird als Minimum vorausgesetzt, besser WPA2.
- Änderung der Standard-Konfiguration, in der die Geräte ausgeliefert werden (Passwort!)
- Aussenden der SSID-Kennung verhindern
- Namen der SSID ändern
- Filterung von MAC-Adressen
- Deaktivieren von DHCP

Die Kirchenverwaltung hat die Fa. NorCom (Anbieter von Sicherheitslösungen für den IT-Bereich) vor einiger Zeit mit einer schriftlichen Ausarbeitung zu diesem Thema beauftragt, die bei Herrn Grellmann angefordert werden kann. Dort werden die erforderlichen Maßnahmen eingehender beschrieben als in dieser FAQ.

Ansprechpartner: Regionalverwaltung

3.1 In welchen Varianten ist der Intranet-Zugang verfügbar?

Den Intranet-Zugang gibt es in zwei Varianten:

Einzelplatz-Lösung

Firewall

Eine *Firewall* ist eine Sicherheitsvorkehrung, die einzelne Computer oder ganze Netzwerke vor unberechtigten Zugriffen aus dem Internet abschirmt.

Auf Einzelplatz-Computern wird der Intranet-Zugang mit Hilfe einer Zusatzsoftware (VPN-Client) ermöglicht. Die benötigte Software befindet sich zusammen mit der von der EKHN empfohlenen Firewall- und Antivirensoftware auf der EKHN-Intranet-CD, die mit den im Kapitel 2.12 aufgeführten Formularen bei der Kirchenverwaltung angefordert werden kann. Diese CD ist seit April 2006 in einer aktualisierten Version (V3.0-2006) verfügbar. Wichtigste Neuerung: Die Verbindungsaufbau (VPN-Tunnel) zum Intranet ist jetzt auch über Router möglich. Es handelt sich weiterhin um eine reine Einzelplatzlösung. Die Anbindung ganzer Netzwerke mit Hilfe der Software-

Lösung ist nicht zulässig und technisch nicht möglich. Bei Neuinstallation des VPN-Clients sollte nur noch diese neue Version verwendet werden.

Netzwerk-Lösung

Wenn in Ihrer Dienststelle mehrere Computer miteinander vernetzt sind, ermöglicht die Gateway-Lösung auf allen Computern den Zugang zum Internet **und** Intranet. Die umständliche Prozedur des Verbindungsaufbaus entfällt, da das Gateway permanent mit dem Internet und Intranet verbunden ist. Zudem wird auf den einzelnen Computern keine Firewall mehr benötigt, da das Gateway eine zentrale Firewall eingebaut hat und das lokale Netzwerk damit nach außen abschirmt. Bisher war für die Gateway-Lösung die Installation eines zusätzlichen Computers (Linux-Gateway) erforderlich. Diese Lösung wird nun durch die „Appliance"-Lösung in Form eines kleinen Gerätes, ähnlich einem Router, abgelöst. Ein zusätzlicher Computer für das Linux-Gateway ist nicht mehr erforderlich. Diese neue Lösung für kleine Netzwerke wird über die Kirchenverwaltung beauftragt und kostet bei Neuinstallation 1.075 € und beim Austausch eines bestehenden Linux-Gateways 600 €, jeweils inkl. MwSt. . Damit ist die neue Appliance-Lösung preisgünstiger als die alte Variante mit dem Linux-Gateway.

Ansprechpartner: Kirchenverwaltung

Wenn der PC nicht älter ist als zwei Jahre, liegt in der Regel eine ausreichende Leistungsfähigkeit vor.

3.2 Erfüllt unser PC die Systemvoraussetzungen für die Teilnahme am Intranet?

Als Faustregel gilt: Wenn der PC innerhalb der letzten beiden Jahre angeschafft wurde, liegt eine ausreichende Leistungsfähigkeit vor.

Die von der Kirchenverwaltung festgelegten Systemvoraussetzungen für die Teilnahme am Intranet und die Bezuschussung im Rahmen des Investitionsprogramms finden Sie hier:

http://www.ekhn.de/intranet/hardware.htm

Ansprechpartner: Kirchenverwaltung

Für die Installation der aktuellen Intranet-CD wird als Betriebssystem Windows 2000 (SP4) oder Windows XP (SP2) benötigt.

3.3 Unter welchen Betriebssystem-Versionen kann der Intranet-Zugang installiert werden?

Die dritte und vierte Version der VPN-Software (siehe Kapitel 1.10) erfordert als Betriebssystem Windows 2000 (SP4) oder Windows XP (SP2). Ältere Betriebssystem-Versionen werden nicht mehr unterstützt. Beim Einsatz der Gateway-Lösung für kleine Netzwerke spielt das auf Anwenderseite eingesetzte Betriebssystem und die Betriebssystemversion keine Rolle.

3.4 Unser PC funktioniert nicht richtig.

Bei kleinen Problemen hilft es manchmal, die betroffenen Geräte aus- und wieder einzuschalten (Neustart).

Bei größeren Problemen kann die Neuinstallation des Betriebssystems und aller Programme notwendig sein. Oft ist das effektiver als eine stundenlange Fehlersuche. Führen Sie vorher unbedingt eine Datensicherung durch!

Wenn Ihnen die Hinweise in dieser FAQ nicht weitergeholfen haben, setzen Sie sich mit einem Fachmann in Verbindung.

Im Anhang dieser Broschüre finden Sie Adressen von Fachfirmen, die neben fundiertem EDV-Fachwissen über Kenntnisse des EKHN-Intranets und der

kirchlichen Strukturen verfügen.

3.5 Welche Grundkonfiguration ist für den Intranet-Zugang erforderlich?

Wir empfehlen eine wie hier beschriebene Grundkonfiguration des Computers.

Die Installation des VPN-Clients für den Verbindungsaufbau zum Intranet ist mit vielen „Fallstricken“ verbunden. In den meisten Fällen gelingt die Installation, wenn eine wie folgt beschriebene Konfiguration vorliegt:

Online-Zugang

Als Internetzugang wird T-DSL Business in Verbindung mit einer T-Online-Flatrate empfohlen. Die Installation des T-Online-Startcenters ist nicht notwendig. Wenn kein Router verwendet wird (der selbst für den Verbindungsaufbau zum Internet sorgt), wird empfohlen die Einwahl ins Internet mit Hilfe einer DFÜ-Verbindung zu realisieren. Noch komfortabler kann der Verbindungsaufbau erfolgen, wenn die Parameter für den Verbindungsaufbau mit dem Internet direkt unter „Eigenschaften“ des VPN-Clients hinterlegt werden. Der Vollständigkeit halber wird darauf hingewiesen, dass das Speichern von Kennwörtern ein Sicherheitsrisiko darstellt und laut Sicherheitsrichtlinie der EKHN nicht zulässig ist.

Hinweise zur Konfiguration eines Routers (falls vorhanden)

Der Verbindungsaufbau zum Intranet mit dem VPN-Clients für Einzelplatzcomputer ist erst ab Version V3.0-2006 der Intranet-CD auch über Router möglich.

Bei der Konfiguration von Adressbereichen auf dem Router bzw. DHCP-Server dürfen lokal keine IP-Adressen aus den Bereichen 192.168.5.xxx, 192.168.100.xxx und 192.168.201.xxx verwendet werden, da es sich hier um reservierte Bereiche handelt.

DHCP

ist die Abkürzung für *Dynamic Host Configuration Protocol*. *DHCP* ist ein System, das die dynamische Zuweisung von IP-Adressen an Computer und andere Netzwerkgeräte (z.B. Drucker) regelt.

Betriebssystem

Als Betriebssystem wird Windows 2000 (SP4) oder Windows XP Professional (SP2) empfohlen.

Sicherheitsupdates

sind regelmäßig von Microsoft zur Verfügung gestellte Aktualisierungen für die Windows-Betriebssysteme, mit denen Sicherheitslücken geschlossen werden.

Installieren Sie die von Microsoft zur Verfügung gestellten Sicherheitsupdates oder aktivieren Sie die Funktion „Automatische Updates“.

Da (wie unten beschrieben) eine Desktop-Firewall eingesetzt werden soll, kann der Dienst „Windows-Firewall/Gemeinsame Nutzung der Internetverbindung“ beendet und deaktiviert werden.

Deaktivieren Sie darüber hinaus alle nicht für den Intranetzugang benötigten Netzwerkverbindungen.

Empfohlene Softwareausstattung

Die aktuelle Office-Version ist Microsoft Office 2003. Für die Funktionsfähigkeit des Intranet-Zugangs spielt die verwendete Office-Version keine Rolle.

Kaspersky

ist die Herstellerfirma der von der EKHN empfohlenen Sicherheitssoftware. Die Software befindet sich auf der Intranet-CD.

Zusätzlich benötigte Programme

Firewall

Eine Firewall verhält sich wie ein Schutzschild, das Ihren Computer im öffentlichen Internet unsichtbar macht und vor unberechtigten Zugriffen schützt. Die von der EKHN empfohlene Desktop-Firewall „Kaspersky Anti-

Hacker“ befindet sich auf der Intranet-CD und ist für 17 € über die Kirchenverwaltung zu beziehen.
Wenn in Ihrer Dienststelle die Gateway-Lösung für dienstliche Netzwerke zum Einsatz kommt, ist die Installation einer Desktop-Firewall nicht zwingend erforderlich.

Antivirenprogramm

Darüber hinaus benötigen Sie ein Antivirenprogramm, das den Computer vor Viren und anderen destruktiven Programmen schützt.

Die von der EKHN empfohlene Firewall-Software „Kaspersky Antivirus“ befindet sich auf der Intranet-CD und ist für 17 € über die Kirchenverwaltung zu beziehen.

PDF

Das *Portable Document Format* ist ein Dateiformat, das es ermöglicht ein Dokument unter Beibehaltung seines Layouts auf unterschiedliche Systeme zu übertragen. Zum Anzeigen und Drucken einer PDF-Datei ist der kostenlos erhältliche Acrobat-Reader erforderlich.

Acrobat-Reader

Um PDF-Dateien anzuzeigen und zu drucken wird der Acrobat-Reader benötigt. Auf der Informationsplattform im Intranet werden eine Vielzahl an Dokumenten in Form von PDF-Dateien bereitgestellt; darüber hinaus erfolgt die Druckausgabe in KFM-Web und netKIM im PDF-Format.

Der Acrobat-Reader befindet sich ebenfalls auf der Intranet-CD. Möglicherweise stehen mittlerweile aktuellere Versionen im Internet zum Download bereit: http://www.adobe.de/ .

Popups

Als *Popups* bezeichnet man kleine Fenster, die beim Besuch einer Webseite – meist ungewollt - aufspringen um Informationen oder Werbung anzuzeigen.

Popupblocker deaktivieren

KFM-Web erfordert noch eine weitere Systemvoraussetzung: Sie müssen den Popupblocker entweder generell oder speziell für die KFM-Intranet-Adresse deaktivieren, da in KFM-Web verschiedene Dialoge und Fenster in Form von Popup-Fenstern angezeigt werden.

Datensicherung

Erstellen Sie unbedingt regelmäßige Datensicherungen um für den Fall eines Datenverlustes (z.B. durch Festplattendefekt, Virus, Einbruchdiebstahl, versehentliches Löschen usw.) abgesichert zu sein! Datensicherungen sollten auf einem externen Sicherungsmedium (DVD, CD, USB-Stick, externe Festplatte usw.) erfolgen. Für die Sicherung von Servern in Netzwerkumgebungen wird ein Bandlaufwerk empfohlen. Die Sicherungsmedien sollten räumlich getrennt und unter Verschluss aufbewahrt werden.

Sicherung mit Hilfe von Imaging-Verfahren

Eine noch höhere Datensicherheit wird erreicht, wenn Sie mit Hilfe geeigneter Werkzeuge wie Ghost oder Acronis True Image eine Abbildsicherung (Image) Ihrer Festplatte anfertigen und diese Sicherung auf einem externen Medium speichern. Für den Fall, dass die Windows-Installation oder ein sonstiges Programm Schaden nimmt, kann der PC mit dieser Methode mit geringem Zeitaufwand jederzeit wieder in einen als funktionierend bekannten Zustand versetzt werden.

3.6 Welche Versionen gibt es von der Intranet-CD?

Es gibt mittlerweile vier Versionen der Intranet-CD:

- Gelbe Erstausgabe mit dem @-Zeichen.
- Zweite Version als gebrannte, unbeschriftete CD
- Dritte Version vom Oktober 2004

- Vierte Version V3.0-2006 vom April 2006 (lila CD, siehe Abbildung)

Die dritte und vierte Version enthält einen stark verbesserten Installations-Assistenten sowie eine besser geeignete und leichter zu bedienende Firewall- und Antivirensoftware (Kaspersky AntiHacker 1.5 und Kaspersky AntiVirus Personal 5.0).

Als Betriebssystem werden Windows 2000 (SP4) oder Windows XP (SP2) vorausgesetzt. Ältere Betriebssystemversionen werden nicht mehr unterstützt.

Abb.: Aktuelle Version der Intranet-CD

Wenn Sie bereits über Zugang zum Intranet verfügen, müssen Sie nicht unbedingt auf die neue Version aktualisieren.

Wenn Sie eine Neuinstallation des Intranet-Zugangs vornehmen oder Ihre bisherige Installation nicht richtig funktioniert, installieren Sie die aktuelle Version.

Die CD kann mit einem der folgenden Formulare bei der Kirchenverwaltung angefordert werden. Bei gleichzeitiger Beantragung der Lizenzen für die Kaspersky-Firewall und das Kaspersky-Antivirenprogramm entstehen Kosten in Höhe von 17 €. Die Lizenz muss nach einem Jahr verlängert werden.

Antragsformular Intranet
http://www.ekhn.de/intranet/download/anmeldung_intranet_einzel.pdf

Antrag auf Änderung der Zugangsart bzw. Anforderung der neuen Intranet-CD bei bereits vorhandenem Intranet-Zugang
http://www.ekhn.de/intranet/download/anmeldung_intranet_einzel_dsl.pdf

Ansprechpartner: Kirchenverwaltung

3.7 Woran ist zu erkennen welche Version des VPN-Clients auf meinem Computer installiert ist?

Wenn Sie die Einwahl über eine Desktop-Verknüpfung „EKHNVPN“ vornehmen und bei der Einwahl ein Dialog mit dem EKHN-Logo angezeigt wird (siehe Kapitel 3.9), dann haben Sie die aktuelle Version V3.0-2006 im Einsatz.

Wenn Sie die Einwahl über eine Desktop-Verknüpfung „Tunnel aufbauen“ vornehmen und sich bei der Einwahl für einige Sekunden ein Fenster öffnet, in dem auf schwarzem Hintergrund in weißer Schrift Programmbefehle ablaufen, haben Sie eine ältere Version im Einsatz.

3.8 Welche Neuerungen bringt die Version V3.0-2006 der Intranet-CD?

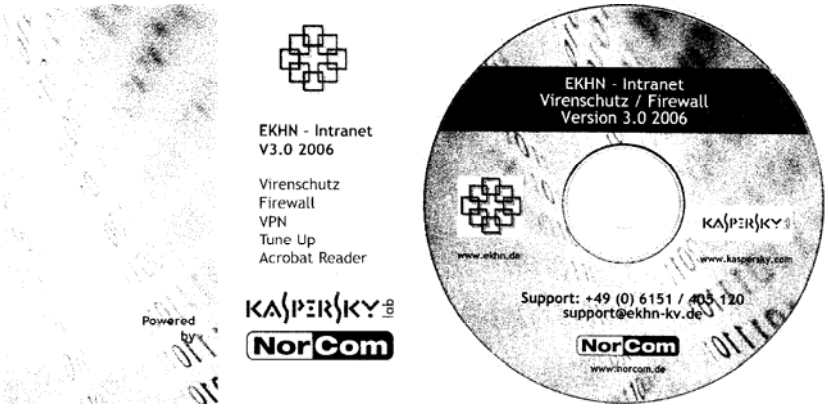


Abb.: Aktuelle Version der Intranet-CD

Die vorliegende Version der Intranet-CD ist nur noch für die Betriebssysteme Windows 2000 und Windows XP geeignet. Ältere bzw. andere Betriebssysteme werden nicht mehr unterstützt.

Sollte auf dem Computer eine ältere oder andere Version des VPN-Clients installiert sein, muss diese vor der Installation der neuen Version wie in der Installationsanleitung beschrieben entfernt werden.

Die seit April 2006 vorliegende Version der Intranet-CD (V3.0-2006) enthält neben der von der EKHN empfohlene Antiviren- und Firewallsoftware auch die aktuellen Service-Packs für die gängigen Windows-Betriebssysteme, den kostenlosen Acrobat Reader zum Anzeigen elektronischer Dokumente, sowie eine neue Version des VPN-Clients. Da der VPN-Client die eigentliche Zugangssoftware zum Intranet darstellt, soll in diesem Kapitel näher auf die diesbezüglichen Neuerungen eingegangen werden:

Die größte Schwierigkeit vorangegangener Versionen des VPN-Clients war, dass aus technischen Gründen keine Verbindung zum Intranet über einen Router hergestellt werden konnte und die in Windows integrierte Firewall vollständig deaktiviert werden musste.

Die aktuelle Version erlaubt nun endlich den Verbindungsaufbau über Router, allerdings nur von einem einzelnen Computer im lokalen Netzwerk aus. Die gleichzeitige Einwahl mehrerer Computer in das Intranet ist auf diesem Weg nicht möglich (siehe Kapitel 2.10, Anbindung von Netzwerken).

Das Deaktivieren der Windows-Firewall ist an sich nicht mehr zwingend notwendig. Da jedoch die Installation der Kaspersky-AntiHacker-Firewall empfohlen wird und jeweils nur eine Firewall installiert bzw. aktiviert sein sollte, ist – sofern die Kaspersky-Firewall tatsächlich verwendet wird - ein Deaktivieren der Windows-Firewall anzuraten.

Für die VPN-Verbindung legt das Setupprogramm eine Netzwerkverbindung „EKHNVPN“ und eine Verknüpfung auf dem Desktop an. Um sich ins Intranet einzuwählen, stellt man zunächst eine Verbindung zum Internet her, klickt dann auf die Verknüpfung „EKHNVPN“ und gibt dort Benutzernamen und Kennwort ein. Wem das zu umständlich ist, der kann die Parameter für den Verbindungsaufbau mit dem Internet direkt unter „Eigenschaften“ des VPN-Clients hinterlegen. Der Vollständigkeit halber sei der Hinweis gegeben, dass es laut Sicherheitsrichtlinie der EKHN nicht zulässig ist, die Option „Kennwort speichern“ zu aktivieren.

Ansprechpartner: Regionalverwaltung

3.9 Welches Passwort muss in dem DFÜ-Dialog zur Verbindungsherstellung mit „EKHNVPN“ (neue Intranet-CD) eingegeben werden?

DFÜ-Verbindung

DFÜ ist die etwas veraltete Abkürzung für *Datenfernübertragung*. *DFÜ-Verbindungen* ermöglichen die Einwahl in ein Computernetzwerk. In der Regel ist die Angabe eines Benutzernamens und Kennworts notwendig.

Wenn Sie die aktuelle Version der VPN-Software (V3.0-2006) installiert haben, müssen Sie für den Verbindungsaufbau zum Intranet einen Benutzernamen und ein Kennwort eingeben wie in folgendem Dialog gezeigt:

SUSE OpenExchange

ist die zentrale Mailserversoftware, die das Senden und Empfangen von E-Mails @ekhnnet.de steuert.

Als Benutzernamen geben Sie hier Ihre ekhnnet-Kennung ein (z.B. „ekhnnet00123“). Als Kennwort geben Sie das Kennwort ein, mit dem Sie sich in „SUSE OpenExchange“ an Ihrem E-Mail-Postfach anmelden.

Das Feld „Anmeldedomäne“ bleibt leer.

Ansprechpartner: Kirchenverwaltung

3.10 Unser Intranet-Zugang funktioniert nicht richtig. Wo liegen häufige Fehlerquellen?

Erfahrungsgemäß gelingt die Installation der VPN-Software und der beiden Sicherheitsprogramme, wenn eine ganze Reihe von Voraussetzungen gegeben sind und der PC nach dem empfohlenen Schema konfiguriert ist. Eine solche Standard-Konfiguration ist im Kapitel 3.5 beschrieben

Die Gateway-Lösung für kleine Netzwerke ist weniger anfällig für Störungen und Kompatibilitätsprobleme.

Häufige Fehlerquellen:

1. Bei Verwendung einer älteren Version der VPN-Software/Intranet-CD

- Die in das Betriebssystem Windows XP SP2 integrierte Firewall ist aktiviert. Diese Firewall ist nicht mit dem EKHN-Intranet kompatibel. Beenden und deaktivieren Sie den Dienst „Windows-Firewall/Gemeinsame Nutzung der Internetverbindung“. Es reicht nicht aus, die Windows-Firewall auf „inaktiv“ zu schalten! Erst die aktuelle Version des VPN-Clients erlaubt einen Verbindungsaufbau zum Intranet auch bei aktivierter Windows-Firewall.

BIOS

Das *Basis Input Output System* des Computers übernimmt nach dem Einschalten des Rechners die Steuerung der Grundkomponenten des Computers.

- Ihr PC ist mit einer aktivierten Netzwerkverbindung (z.B. Netzwerkkarte) ausgestattet. Bei dem VPN-Client bzw. der Intranet-CD handelt es sich um eine Einzelplatzlösung, die für Netzwerk-PC’s nicht geeignet ist. Deaktivieren Sie ggf. alle Netzwerkverbindungen, die nicht für den Verbindungsaufbau ins Internet benötigt werden. Wenn Ihr PC mit einer On-Board-Netzwerkkarte ausgestattet ist und diese nicht zum Verbindungsaufbau mit dem Internet benötigt wird, deaktivieren Sie diese On-Board-Netzwerkkarte auch im BIOS.

- Sie haben einen Router oder einen WLAN-Router im Einsatz, mit dem Sie mehreren PC’s den Zugang zum Internet über einen DSL-Anschluss ermöglichen. Aus technischen Gründen können ältere Versionen des VPN-Clients (erst ab Version V3.0-2006 möglich) über einen Router keine Verbindung zum Intranet herstellen. Um dienstliche Netzwerke mit dem Intranet zu verbinden, benötigen Sie die Gateway-Lösung für kleine Netze, die über die Kirchenverwaltung beantragt werden kann.

- Ab Version V3.0-2006 des VPN-Clients ist es technisch möglich, auch über einen Router eine Verbindung (Tunnel) zum Intranet aufzubauen. Allerdings handelt es sich hierbei weiterhin um eine reine Einzelplatzlösung. Die Anbindung ganzer Netzwerke auf diesem Weg ist weiterhin nicht zulässig und technisch nicht möglich.

2. Bei Verwendung der neuen Intranet-CD V3.0-2006

- Wenn Sie die neueste Version der VPN-Software installiert haben (V3.0-2006), müssen Sie bei der Einwahl ins Intranet eine Benutzerkennung und ein Passwort eingeben. Prüfen Sie an Hand von Kapitel 3.9 in dieser Broschüre, ob Sie die richtigen Anmeldeinformationen eingegeben haben.

- Sie haben die neueste Version des VPN-Clients installiert (V3.0-2006) und erhalten folgende Fehlermeldung:

  Der Verbindungsversuch ist fehlgeschlagen, da die Datenverschlüsselung fehlerhaft war. (Fehler 768).

  Dieser Fehler tritt dann auf, wenn Sie die neue Version des VPN-Clients einfach „über“ die alte Version installiert haben. Abhilfe: Deinstallieren Sie die Vorgängerversion wie in der neuen Installati onsanleitung beschrieben.

- Stellen Sie sicher, das im eigenen Netzwerk keine IP-Adressen aus den (reservierten) Bereichen

  192.168.5.xxx
  192.168.100.xxx

192.168.201.xxx

verwendet werden. Dazu müssen Sie ggf. Ihren Router bzw. Ihren DHCP-Server umkonfigurieren. Sehen Sie dazu im Handbuch Ihres Routers nach oder kontaktieren Sie Ihren IT-Betreuer.

- Sie haben bei der Installation des VPN-Clients einen falschen Benutzernamen oder ein falsches Passwort eingegeben und die Installation ist anschließend mit einer Fehlermeldung abgebrochen. Ein erneutes Installieren des VPN-Clients ist jedoch nicht möglich, da die Option „VPN-Software“ nicht mehr auf der Oberfläche des Installationsassistenten angezeigt wird.
  Abhilfe: Stellen Sie zunächst sicher, dass Sie im Besitz der korrekten Zugangsdaten zum Intranet sind (erfragen Sie diese ggf. bei der EKHN), löschen anschließend die Netzwerkverbindung „EKHN-VPN“ und installieren die VPN-Software anschließend neu. Nach dem Löschen der Netzwerkverbindung „EKHNVPN“ wird die Option zum Installieren der VPN-Software wieder auf der Oberfläche des Installationsassistenten angezeigt.

3. Alle Versionen

- Nach der Einwahl ins Internet wurde nicht auf „VPN-Aufbau“ geklickt.

- Sie sind auf Windowsebene mit Benutzerrechten am PC angemeldet. Der Intranet-Zugang ist nur mit Administratoren-Rechten möglich.

- Wenn Sie eine andere Firewall als Kaspersky AntiHacker von der Intranet-CD einsetzen, haben Sie dort unter Umständen nicht die erforderlichen IP-Ausnahmen korrekt eingetragen.

- Sie haben versehentlich oder beabsichtigt in der Firewall Programmen wie dem Internet Explorer, Outlook oder bestimmten, für den Internetzugang erforderlichen Systemprogrammen den Zugriff auf das Internet verweigert. Setzen Sie ggf. die Einstellungen in der Firewall auf den Zustand nach der Erstinstallation zurück. Empfehlung: Die auf der neuen Intranet-CD befindliche Firewall (Kaspersky AntiHacker 1.5) ist so vorkonfiguriert, dass für die erforderlichen Systemprogramme bereits Ausnahmen definiert sind. Dadurch konfrontiert Sie die Firewall nicht mehr mit so vielen Fragen, welchen Programmen der Zugriff auf das Intranet erlaubt werden soll.

- Versuchen Sie ggf. testweise für wenige Sekunden, die Verbindung zum Intranet bei deaktivierter Firewall herzustellen, um eine Fehlkonfiguration der Firewall als Ursache auszuschließen. Achtung: Das Deaktivieren der Firewall stellt ein erhebliches Sicherheitsrisiko dar!

Proxy-Server

Der Begriff *Proxy* bedeutet soviel wie „Stellvertreter“ und bezeichnet einen Server, der zwischen den Computer des Benutzers und das Internet geschaltet ist. *Proxy-Server* sind für die Zwischenspeicherung häufig abgerufener Webseiten

- In den Verbindungseinstellungen Ihrer DFÜ-Verbindung bzw. in den Internetoptionen ist ein Proxy-Server eingetragen, über den keine Kommunikation mit dem Intranet möglich ist. Das ist z.B. bei Freenet oder u.U. bei Verwendung des T-Online-Startcenters der Fall.

- Ihr PC ist an eine Telefonanlage mit integrierter Firewall angeschlossen (etwa Eumex 520 PC). Deaktivieren Sie die integrierte Firewall der Telefonanlage und benutzen Sie die auf der Intranet-CD mitgelieferte Kaspersky-Firewall „Kaspersky AntiHacker“).

zuständig und können dadurch den Seitenaufbau beschleunigen.

SP (Servicepack)

Ein *Servicepack* ist eine Zusammenstellung einzelner Aktualisierungen und Updates für ein Betriebssystem oder Computerprogramm.

NTBA

Abkürzung für *Network Termination of Basic Access* - Adapter zwischen dem Netz der Deutschen Telekom und dem privaten S0-/ISDN-Bus (Telefonanlage). Der NTBA besteht aus einer von der Telekom gestellten, grau-weißen Box in der Größe einer Zigarrenkiste.

Desktop-Firewall

Mit *Desktop-Firewall* bezeichnet man eine auf einem einzelnen Computer installierte Sicherheitssoftware, die den Computer gegenüber unberechtigten Zugriffen aus dem Internet absichert.

- Wenn auf Ihrem PC unter Windows XP SP1 das „Advanced Network Pack“ installiert ist, kommt es möglicherweise zu einer Unverträglichkeit mit dem VPN-Client. Wenn die Deinstallation des „Advanced Network Pack“ nicht hilft, versuchen Sie zunächst die Installation des SP2 für Windows XP. Hilft auch das nicht, ist die Neuinstallation des Betriebssystems notwendig.

- In Einzelfällen wurde festgestellt, dass manche Treiberversionen für Netzwerk- oder ISDN-Karten nicht mit dem VPN-Client kompatibel sind.

- In Einzelfällen wurde festgestellt, dass ein Verbindungsaufbau zum Intranet nicht möglich ist, wenn der PC über die USB-Schnittstelle direkt mit der Telefonanlage verbunden ist. Verbinden Sie den PC ggf. über eine klassische ISDN-Karte (z.B. AVM Fritz!) direkt mit der s0-Schnittstelle Ihrer Telefonanlage oder Ihres NTBA. Wenn Sie einen DSL-Anschluss haben, verbinden Sie die Netzwerkkarte des PC’s mit dem DSL-Modem.

3.11 Funktioniert der Intranet-Zugang auch unter Service Pack 2 für Windows XP?

Ja, aber: wenn Sie eine ältere Version der VPN-Software einsetzen, müssen Sie den Dienst „Windows-Firewall/Gemeinsame Nutzung der Internetverbindung“ deaktivieren und eine eigene Firewall installieren. Die von der EKHN empfohlene Firewall (Kaspersky AntiHacker) befindet sich auf der Intranet-CD.

3.12 Können wir die in das Service Pack 2 für Windows XP integrierte Firewall verwenden?

Die in das Betriebssystem integrierte Firewall des SP2 ist mit früheren Versionen des VPN-Clients nicht kompatibel. Erst die aktuelle Version des VPN-Clients erlaubt einen Verbindungsaufbau zum Intranet auch bei aktivierter Windows-Firewall. Die Installation der auf der Intranet-CD mitgelieferten Kaspersky-AntiHacker-Firewall wird empfohlen.

3.13 Welche Ausnahmen müssen in der Firewallsoftware für das Intranet konfiguriert werden?

Wenn Sie die von der Kirchenverwaltung empfohlene Firewallsoftware „Kaspersky-AntiHacker 1.5“ von der Intranet-CD einsetzen, müssen keine Ausnahmen konfiguriert werden.

Wenn eine andere Desktop-Firewall verwendet werden soll, müssen unter Umständen folgende Ausnahmen erstellt werden. Weitere Hinweise dazu entnehmen Sie bitte dem Handbuch der entsprechenden Firewallsoftware.

217.6.23.69
192.168.xxx.xxx. (Adressbereich 192.168.1.1 bis 192.168.255.255)

3.14 Intranetzugang über Router

Mit älteren Versionen des VPN-Clients ist aus technischen Gründen kein Verbindungsaufbau bzw. Tunnelaufbau zum Intranet möglich, wenn ein Router verwendet wird und die Netzwerkkarte nicht direkt mit dem DSL-Modem verbunden ist. Erst die aktuelle Version des VPN-Clients (Version V3.0-2006) ermöglicht den Verbindungsaufbau zum Intranet auch über Router.

Allerdings handelt es sich hierbei um eine reine Einzelplatzlösung. Die Anbindung ganzer Netzwerke auf diesem Weg ist nicht zulässig und technisch nicht möglich.

Linux

Linux ist ein freies Betriebssystem und wird von manchen als Alternative zu Windows verstanden. Ein Betriebssystem ist eine Sammlung grundlegender Programme, die ein Computer zum Arbeiten benötigt.

3.15 Ist ein Intranet-Zugang auch unter Linux möglich?

Die von der Kirchenverwaltung der EKHN empfohlenen Betriebssysteme sind Windows 2000 und Windows XP. Für nicht auf Windows basierende Betriebssysteme ist kein Support vorgesehen. Eine Installations-CD für Linux ist nicht verfügbar. In Ausnahmefällen kann der Intranet-Zugang jedoch im Rahmen einer Fernwartungssitzung manuell durch die Kirchenverwaltung konfiguriert werden.

Wenn Sie die Gateway-Lösung für kleine Netzwerke im Einsatz haben, spielt das verwendete Betriebssystem keine Rolle, das sich die Gateway-Lösung wie ein Router verhält.

Ansprechpartner: Kirchenverwaltung

Zertifikat

Ein *Zertifikat* ist ein elektronischer Ausweis, der die Identität einer Person oder eines Zugangscodes bestätigt.

Lizenzschlüssel

Ein *Lizenzschlüssel* ist ein Schlüssel, mit dessen Hilfe sichergestellt wird dass eine Software nur dann benutzt werden kann, wenn sie vom Anwender ordnungsgemäß lizenziert bzw. erworben wurde.

3.16 Während der Installation schlägt das Herunterladen des VPN-Zertifikats und/oder der Lizenzschlüssel für Kaspersky AntiHacker und/oder Kaspersky Firewall fehl.

Vorbemerkung

Wenn Sie die VPN- und Sicherheitssoftware zum ersten Mal installieren oder wenn Sie ein Update/Neuinstallation durchführen und das VPN-Zertifikat und die Lizenzschlüssel nicht wie unten beschrieben im Ordner „Eigene Dateien“ bereitgestellt haben, wird Sie der Installationsassistent im Verlauf der Installation zur Eingabe von Benutzernamen und Passwort auffordern, die Zertifikatsdatei und Lizenzschlüssel anschließend aus dem Internet herunterladen und danach im Ordner „Eigene Dateien“ speichern.

Mögliche Fehlersituationen

Obwohl Sie den richtigen Benutzernamen und das richtige Passwort eingegeben haben, schlägt das Herunterladen der Lizenzschlüssel fehl mit dem Hinweis, Sie mögen sich mit der EKHN in Verbindung setzen. Die Installation der AntiHacker-Firewall und des AntiVirus-Programms ist dann nicht möglich.

Dieses Verhalten tritt auf, wenn Sie die Installation des VPN-Clients und das Herunterladen von Zertifikat und Lizenzschlüssel aus dem Internet ein weiteres Mal versuchen. Dieses Herunterladen ist nur einmal möglich, kann aber von der Kirchenverwaltung erneut frei geschaltet werden.

Eine andere Ursache kann sein, dass die Lizenzschlüssel für Sie nicht zum Download bereitgestellt wurden, weil Sie bei der Anmeldung zum Intranet nicht angekreuzt haben dass Sie die Kaspersky-Software bestellen möchten.

Tipp: Sichern Sie die drei Dateien sofort nach der Installation auf Diskette oder CD. Die betreffenden Dateien werden standardmäßig im Ordner „**Eigene Dateien**“ abgelegt:

- **anti_hacker.key** (Lizenzdatei für die Kaspersky-Firewall)
- **ekhnnet00000.ekhn-kv.de.p12** (Zertifikat für den VPN-Client, an Stelle der 00000 steht Ihr Benutzercode)
- **personal.key (**Lizenzdatei für Kaspersky AntiVirus)

Sollten Sie VPN-Client, Kaspersky AntiHacker oder Kaspersky AntiVirus zu einem späteren Zeitpunkt neu installieren wollen (z.B. weil Sie einen neuen PC erworben haben oder die Neuinstallation des Betriebssystems erforderlich war), müssen Sie diese drei Dateien manuell in den Ordner „Eigene Dateien“ kopieren, da das Herunterladen aus dem Internet nur einmal möglich ist.

Wenn das Installationsprogramm die erforderlichen Zertifikate bzw. Lizenzschlüssel im Ordner „Eigene Dateien“ ermitteln konnte, wird auf den Download aus dem Internet verzichtet (dieser würde unter Umständen fehlschlagen, weil der Download nur einmal möglich ist).

Veraltetes VPN-Zertifikat

Wenn Ihr VPN-Zertifikat mit einer sehr alten Version des VPN-Clients ausgeliefert wurde, müssen Sie unter Umständen ein aktuelles VPN-Zertifikat bei der Kirchenverwaltung beantragen.

Ansprechpartner: Kirchenverwaltung

3.17 Wie schützen wir unseren PC vor Angriffen aus dem Internet und durch andere destruktive Programme?

Sicherheitsempfehlungen

Beachten Sie diese Hinweise um Ihren Computer vor Schädlingen zu schützen.

- Installieren Sie eine Firewall.
- Installieren Sie ein Antivirenprogramm und halten Sie die Virendefinitionen stets auf einem aktuellen Stand.
- Installieren Sie die von Microsoft regelmäßig zur Verfügung gestellten Sicherheitsupdates bzw. aktivieren Sie die Funktion „Automatische Updates“ des Windows-Betriebssystems.
- Öffnen Sie keine E-Mail-Anlagen unbekannter Herkunft.
- Geben Sie Kennwörter nicht aus der Hand.
- Rufen Sie keine zweifelhaften Webseiten auf.

4.1 Anschriftenverzeichnis der EKHN

Das Anschriftenverzeichnis der EKHN im Intranet beinhaltet die Anschriften von allen Dienststellen und Pfarrern der EKHN und bildet das konventionelle, rote Adressbuch in elektronischer Form ab.

Adressänderungen bitte melden

Damit die Adressen im Anschriftenverzeichnis den aktuellen Stand zeigen, melden Sie Änderungen und Ergänzungen (auch bei Telefonnummern und E-Mail-Adressen) an die Kirchenverwaltung:

Ansprechpartner: Kirchenverwaltung

4.2 Inventar-Verwaltung

Gegenstände von bleibendem Wert bzw. ab einem Anschaffungswert von netto 60 € sind Bestandteil des beweglichen Vermögens der Dienststelle bzw. des Rechtsträgers und damit in einem Inventarverzeichnis zu erfassen. Für die Erstellung und Pflege des Inventarverzeichnisses bieten sich konventionelle Listen oder verschiedene Computerprogramme an. Die von der Kirchenverwaltung empfohlene Inventarisierungssoftware ist **Perfect Inventory®** (http://www.perfect-inventory.de). Das Inventarverzeichnis soll in absehbarer Zeit in das Finanzprogramm **KFM-Web** integriert werden. Daher scheint fraglich, ob der Aufbau eines Inventarverzeichnisses mit **Perfect Inventory®** jetzt noch Sinn macht.

Ansprechpartner: Regionalverwaltung

4.3 netKIM-Gemeindegliederverwaltung

Das Meldewesen ist einer der wichtigsten Bereiche der kirchlichen Datenverarbeitung. Mit **netKIM** steht den Dienststellen in der EKHN eine webbasierte Zugriffsmöglichkeit auf alle Gemeindeglieder der eigenen Kirchengemeinde zur Verfügung. Durch die zentrale Datenhaltung auf einem Großrechner und den Wegfall von Schnittstellen ist die Aktualität der Daten stets gewährleistet.

Neben der Erfassung der kirchlichen Amtshandlungen sind mit **netKIM** Auskünfte, Auswertungen und Statistiken möglich.

Ansprechpartner: Kirchenverwaltung

4.4 netKIM-KIBU

Auf der Grundlage der zum 01.01.2006 in Kraft getretenen Kirchenbuchordnung wurde die Möglichkeit geschaffen eine EDV-gestützte Kirchenbuchführung anzuwenden. (Die neue Kirchenbuchordnung - KBO - findet man im Intranet unter „Service für Mitarbeitende“ und weiter unter „Das Recht der EKHN“).

Gegenwärtig befindet sich **netKIM-KIBU** noch in der Pilotphase, jedoch werden schon ab dem nächsten Jahr die ersten Kirchengemeinden mit dem Führen eines elektronischen Kirchenbuches beginnen. Ab dem 01.01.2008 soll das elektronische Kirchenbuch in allen Kirchengemeinden Anwendung finden.

Da **netKIM-KIBU** Bestandteil von **netKIM** ist, sind die Voraussetzungen zum Einsatz dieses neuen Moduls in nahezu allen Dienststellen bereits gegeben.

Ansprechpartner: Kirchenverwaltung

4.5 KFM-Web (Finanzauskunft)

Mit **KFM-Web** steht allen Kirchengemeinden und Bewirtschaftern die Möglichkeit zur Verfügung, tagesaktuelle Informationen über Haushaltsstände online abzufragen. Der monatliche oder vierteljährliche Versand von Sachbuchauszügen gehört damit der Vergangenheit an. Mit Hilfe von **KFM-Web** können Sachbücher jederzeit und tagesaktuell abgerufen werden.

Rechtsträger

Kirchliche Körperschaften wie Kirchengemeinden, Diakoniestationen und Dekanate werden als *Rechtsträger* bezeichnet. Ein *Rechtsträger* ist Träger von Rechten und Pflichten und kann eine natürliche oder eine juristische Person sein.

Gegenwärtig ist **KFM-Web** ein reines Auskunftssystem. Um Abläufe zu beschleunigen und Doppelarbeit zu vermeiden, soll **KFM** zukünftig die Möglichkeit bieten, Anordnungen direkt vor Ort als „Vormerkung“ zu erfassen. Diese Vormerkungen würden der Regionalverwaltung dann in elektronischer Form vorliegen und müssten nur noch zur Zahlung freigegeben werden.

Für die Kirchengemeinden ist der Zugriff auf die Finanzdaten des eigenen Rechtsträgers beschränkt. Die Zugriffsmöglichkeit kann auf dem Anmeldeformular weiter eingeschränkt werden, beispielsweise wenn die Kita-Leiterin zwar Zugriff auf die Finanzdaten der Kindertagesstätte, nicht aber auf die übrigen Haushaltsstellen der Gemeinde erhalten soll.

Anmeldeformular für KFM-Web
http://192.168.5.6/download/doc/edv/kfm_antrag.doc

Verantwortlicher Ansprechpartner und allgemeine Beratung bei Fragen und Problemen:

Ansprechpartner: Kirchenverwaltung

Wenn Sie Ihr Passwort zu KFM-Web vergessen haben oder allgemeine Fragen und Probleme zu KFM-Web haben:

Ansprechpartner: ECKD

4.6 Winkita On Web

Die Beitragsberechnung und –verwaltung der Kindergartenbeiträge erfolgt in den Regionalverwaltungen mit Hilfe von **Winkita**. Mit **Winkita On Web** werden die Kindertagesstätten in die Lage versetzt, die Daten, die sie in den Erhebungsbögen festgehalten haben, direkt in den Computer einzugeben und über das Intranet an die Regionalverwaltung zu übermitteln.

Dadurch entfallen Doppelstrukturen zwischen der anweisenden und ausführenden Stelle und der Datenfluss zur Regionalverwaltung wird vereinfacht und verbessert.

Ansprechpartner: Kirchenverwaltung

5.1 Dienstliche E-Mail-Adresse

Eine dienstliche E-Mail-Adresse „@ekhn-net.de“ ist Bestandteil jedes Intranet-Zugangs.

IT-Verordnung

Mit der IT-Verordnung soll sichergestellt werden, dass die kirchlichen Aufgaben innerhalb der EKHN mit Hilfe der Informationstechnologie sicher, schnell, wirtschaftlich und dem kirchlichen Auftrag gemäß unter Nutzung gemeinsamer Standards erfüllt werden.

Nach § 11 der IT-Verordnung für die EKHN (Amtsblatt 4/2006, Seite 118 ff) ist Dienstpost von allgemeiner Bedeutung künftig an die zentrale E-Mail-Adresse der jeweiligen Einrichtung, die von der Kirchenverwaltung vergeben wurde, zu richten.
Die dienstlichen E-Mail-Adressen der Kirchengemeinden, Kindertagesstätten und Dekanate sowie deren Mitarbeitenden erkennen Sie an der Endung „@ekhn-net.de“.

Persönliche Dienstpost ist nur an die dienstliche E-Mail-Adresse der Mitarbeiterin oder des Mitarbeiters zu adressieren.

Die dienstlichen E-Mail-Adressen der Mitarbeitenden in den Regionalverwaltungen und bei der Kirchenverwaltung haben die Endung „@ekhn-kv.de“.

Ansprechpartner: Kirchenverwaltung

5.2 Welche E-Mail-Programme können verwendet werden?

Webmail

Als *Webmail* werden Dienste im Internet bezeichnet, die die Verwaltung von E-Mails mit einem Webbrowser ermöglichen. Ein spezielles Mail-Programm wie z.B. Outlook, wird dabei nicht benötigt.

Das Senden und Empfangen von Mails über die dienstliche E-Mail-Adresse erfolgt mit der Webmail-Anwendung **Suse Openexchange**. Diese Webmail-Oberfläche hat den Vorteil, dass keine zusätzliche Software angeschafft, installiert und gewartet werden muss und der Zugriff von jedem Intranet-fähigen Computer aus möglich ist.

Die Authentifizierung erfolgt mittels Benutzernamen und Kennwort. Der Benutzername beginnt in der Regel mit „ekhnnet...“ gefolgt von einer meist fünfstelligen Ziffernfolge.

Dieser Mail-Server wird von der Kirchenverwaltung betrieben. Wenn Ihnen

Ihr Kennwort nicht mehr bekannt ist, nehmen Sie Kontakt mit der Kirchenverwaltung auf.

Ansprechpartner: Kirchenverwaltung

5.3 POP3-Konfiguration von Outlook für den Zugriff auf die dienstliche E-Mail-Adresse

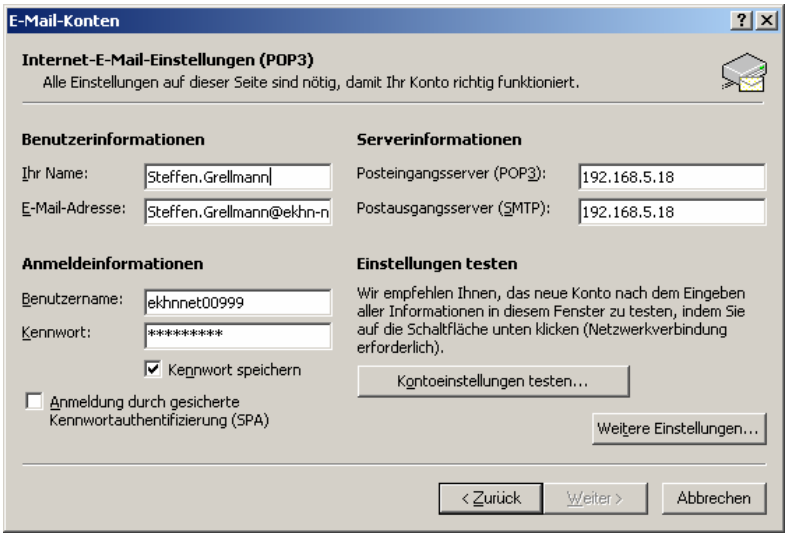
POP3

POP3 (*Post Office Protocol, Version 3*) ist ein Übertragungsprotokoll, über das E-Mails von einem E-Mail-Server abgeholt werden können. Eingegangene Nachrichten werden so lange in einem Postfach auf dem Mailserver gespeichert, bis sie vom Benutzer abgerufen werden.

Wer den Komfort eines vollwertigen E-Mail-Programms in **Suse Openexchange** vermisst, kann mit Outlook über POP3 auf die dienstliche E-Mail-Adresse zugreifen.

Dazu legen Sie in Outlook ein neues E-Mail-Konto wie nachfolgend beschrieben an:

Ihr Name:	Erster Teil der dienstlichen E-Mail-Adresse (bis zum @-Zeichen)
E-Mail-Adresse:	komplette dienstliche E-Mail-Adresse
Benutzername:	ekhnnet-Kennung
Kennwort:	Kennwort
Posteingangsserver (POP3):	192.168.5.18
Postausgangsserver (SMTP):	192.168.5.18



Wenn Sie ausschließlich mit Outlook auf Ihre dienstliche E-Mail-Adresse zugreifen und nicht parallel eine Zugriffsmöglichkeit über die Web-Oberfläche „Suse Openexchange“ benötigen, deaktivieren Sie die Option „Kopie aller Nachrichten auf dem Server belassen“. Wenn Sie diese Option aktiviert lassen, erscheinen neue Mails unter Umständen doppelt im „Posteingang“ von Outlook.

5.4 Unerwünschte Massen-Mails (Spam- bzw. Junk-Mail)

In zunehmendem Maße wird die steigende Anzahl von Spam-Mails beklagt. Unter Spam (auch als „Junk-Mail“ bezeichnet) versteht man den unverlangten, massenhaften Versand von Nachrichten.

Empfehlung

Der Mailserver der EKHN kennzeichnet Spam-verdächtige Mails mit dem Zusatz „SPAM“ in der Betreffzeile, so dass ein manuelles Aussortieren deutlich erleichtert wird.

Wenn die Spam-Mails überhand nehmen, können Sie den Spam-Filter Ihres E-Mail-Programms aktivieren. Eine andere Möglichkeit besteht im Festlegen einer Regel in Outlook, die dafür sorgt dass als „SPAM“ in der Betreffzeile gekennzeichnete Mails in einen separaten Ordner verschoben werden.
Für den Fall dass doch einmal eine ernstgemeinte Mail als Spam behandelt und vom Spam-Filter ausgefiltert wird, empfiehlt sich die regelmäßige Kontrolle des Spam-Ordners.

In gewissem Umfang können Sie selbst dazu beitragen, nicht Opfer von Spam-Attacken zu werden:

Geben Sie Ihre offizielle E-Mail-Adresse möglichst nicht öffentlich im Internet, z.B. in Diskussionsforen, preis. Wenn es unumgänglich ist, die E-Mail-Adresse auf einer Webseite zu veröffentlichen, verändern Sie die Schreibweise, z.B. „Kirchengemeinde.XY [at] ekhn-net.de. Dadurch wird ein automatisches Einlesen Ihrer E-Mail-Adresse in Spam-Verteiler erschwert.

Vorsicht ist auch geboten beim Angeben der E- Mail-Adresse in Webformularen, z.B. bei Online-Bestellungen oder beim Abonnieren von Newslettern.

Alle wichtigen Ansprechpartner im Zusammenhang mit Intranet und Datenverarbeitung auf einen Blick.

6.1 An welche Ansprechpartner kann ich mich wenden?

IT-Fachfirmen:

Firma
ComProfis GmbH
Rheinstr. 66
65185 Wiesbaden
Telefon: 0611-3083712
Telefax: 0611-3414801
E-Mail: schaumburg@comprofis.de
Internet: http://www.comprofis.de

Firma
WL
Wolfgang Leyser
Chemnitzer Straße 1
63110 Rodgau
Telefon: 06106-876420
Telefax: 06106-876421
Mobiltelefon: 0173-6659465
E-Mail: wl@wlcomputer.de

Firma
Worldmatrix
Karl Heinz Klein
Edisonstr. 19
65199 Wiesbaden
Telefon: 0611-41140847
Telefax: 0611-41140848
Mobiltelefon: 0151-15224714
E-Mail: info@worldmatrix.de
Internet: http://www.worldmatrix.de

Kirchlicher Rahmenvertrag für Microsoft-Software

Kirchliche Gemeinschaftsstelle für elektronische Datenverarbeitung
(KIGST)
Ansprechpartner: Manfred Mohr
Strahlenbergerstraße 112
63067 Offenbach am Main
Telefon: 069-6092-126
Telefax: 069-6092-190
E-Mail: pcsc@kigst.de

Druckerwartung:

Es besteht eine Rahmenvereinbarung zu günstigen Konditionen.
Bei Beauftragung Stichwort „Ev. Kirche Wiesbaden“ angeben.

Berolina
Weidenauer Straße 64
57076 Siegen
Telefon: 0271-77 23 70
Telefax: 0271-7 72 37 37
E-Mail: info@berolina-siegen.de
Internet: http://www.berolina.de

6.2 Häufig benötigte Web-Adressen im Intranet

Intranet-Startseite:	http://192.168.5.6/
E-Mail-Server EKHN:	http://192.168.5.16
netKIM:	http://192.168.100.13/framework/netkim
KFM-Web:	https://kfm.ekhn-kv.de/

Hier werden die in dieser Broschüre verwendeten (Fach-)begriffe verständlich erklärt.

6.3 Glossar

BIOS

Das *Basis Input Output System* des Computers übernimmt nach dem Einschalten des Rechners die Steuerung der Grundkomponenten des Computers.

Dekanatsbeauftragte

Diese Funktion wird meist von Ehrenamtlichen oder von Pfarrer(innen) als Zusatzauftrag wahrgenommen. Aufgabe der *Dekanatsbeauftragten* ist die Einführung des Intranets in den Dienststellen der EKHN zu koordinieren und das Zuschussverfahren zu überwachen.

Desktop-Firewall

Mit *Desktop-Firewall* bezeichnet man eine auf einem einzelnen Computer installierte Sicherheitssoftware, die den Computer gegenüber unberechtigten Zugriffen aus dem Internet absichert.

DFÜ-Verbindung

DFÜ ist die etwas veraltete Abkürzung für *Datenfernübertragung*. *DFÜ-Verbindungen* ermöglichen die Einwahl in ein Computernetzwerk. In der Regel ist die Angabe eines Benutzernamens und Kennworts notwendig.

DHCP

ist die Abkürzung für *Dynamic Host Configuration Protocol*. *DHCP* ist ein System, das die dynamische Zuweisung von IP-Adressen an Computer und andere Netzwerkgeräte (z.B. Drucker) regelt.

DSL

(Digital Subscriber Line) ist eine Breitband-Technologie, die über die herkömmliche Telefonleitung hohe Übertragungsraten und einen sehr schnellen Seitenaufbau im Internet ermöglicht. PC und Telefon können gleichzeitig verwendet werden.

FAQ

FAQ ist die Abkürzung für „*Frequently Asked Questions*“, zu deutsch „Häufig gestellte Fragen“.

Firewall

Eine *Firewall* ist eine Sicherheitsvorkehrung, die einzelne Computer oder ganze Netzwerke vor unberechtigten Zugriffen aus dem Internet abschirmt.

Hier werden die in dieser Broschüre verwendeten (Fach-)begriffe verständlich erklärt.

Flatrate

Bei einer *Flatrate* zahlt man einen monatlichen Pauschalbetrag und kann dafür so lange online sein wie man möchte.

Gateway

Ein *Gateway* ist ein Gerät, das unterschiedliche Rechnernetze miteinander verbindet..

IT-Verordnung (ITVO)

Mit der IT-Verordnung soll sichergestellt werden, dass die kirchlichen Aufgaben innerhalb der EKHN mit Hilfe der Informationstechnologie sicher, schnell, wirtschaftlich und dem kirchlichen Auftrag gemäß unter Nutzung gemeinsamer Standards erfüllt werden.

Kaspersky

ist die Herstellerfirma der von der EKHN empfohlenen Sicherheitssoftware. Die Software befindet sich auf der Intranet-CD.

KFM-Web

KFM-Web ist ein Auskunftssystem, mit dem Kirchengemeinden und weitere Einrichtungen tagesaktuelle Informationen über Haushaltsstände und Finanzdaten über eine Web-Oberfläche abrufen können.

LAN

ist die Abkürzung für *Local Area Network. Als LAN* bezeichnet man ein räumlich begrenztes Netzwerk von Computern, meist innerhalb eines Unternehmens oder einer Behörde. Durch so verbundene Computer können Ressourcen wie Internetzugang, Drucker und Software gemeinsam genutzt werden.

Linux

Linux ist ein freies Betriebssystem und wird von manchen als Alternative zu Windows verstanden. Ein Betriebssystem ist eine Sammlung grundlegender Programme, die ein Computer zum Arbeiten benötigt.

Lizenzkey

Ein *Lizenzkey* ist ein Schlüssel, mit dessen Hilfe sichergestellt wird dass eine Software nur dann benutzt werden kann, wenn sie vom Anwender ordnungsgemäß lizenziert bzw. erworben wurde.

netKIM

netKIM ist die in der EKHN eingesetzte Meldewesen- und Gemeindegliederverwaltung. Bei *netKIM* handelt es sich um eine Web-basierte Anwendung, bei der sämtliche Daten auf einem Großrechner im Rechenzentrum gespeichert sind.

netKIM-KIBU

netKIM-KIBU ist ein Zusatzmodul in **netKIM**, das die elektronische Kirchbuchführung mit **netKIM** ermöglicht.

Hier werden die in dieser Broschüre verwendeten (Fach-)begriffe verständlich erklärt.

NTBA

Abkürzung für *Network Termination of Basic Access* - Adapter zwischen dem Netz der Deutschen Telekom und dem privaten S0-/ISDN-Bus (Telefonanlage). Der NTBA besteht aus einer von der Telekom gestellten, grau-weißen Box in der Größe einer Zigarrenkiste.

Outlook

Outlook ist ein weitverbreitetes E-Mail-Programm, mit dem neben dem Senden und Empfangen von E-Mails auch Kontakte und Termine verwaltet werden können. *Outlook* ist Bestandteil des Office-Paketes und nicht zu verwechseln mit *Outlook Express*, das Bestandteil des Windows-Betriebssystems ist.

PDF

Das *Portable Document Format* ist ein Dateiformat, das es ermöglicht ein Dokument unter Beibehaltung seines Layouts auf unterschiedliche Systeme zu übertragen. Zum Anzeigen und Drucken einer PDF-Datei ist der kostenlos erhältliche Acrobat-Reader erforderlich.

Perfect Inventory®

Perfect Inventory® ist ein Programm, das für die Erstellung und Verwaltung des Inventarverzeichnisses verwendet werden kann. Zusatzmodule ermögliche die automatisierte Ermittlung technischer Daten und installierter Programme aller Computer in Netzwerkumgebungen.

POP3

POP3 (*Post Office Protocol, Version 3*) ist ein Übertragungsprotokoll, über das E-Mails von einem E-Mail-Server abgeholt werden können. Eingegangene Nachrichten werden so lange in einem Postfach auf dem Mailserver gespeichert, bis sie vom Benutzer abgerufen werden.

Popups

Als *Popups* bezeichnet man kleine Fenster, die beim Besuch einer Webseite – meist ungewollt - aufspringen um Informationen oder Werbung anzuzeigen.

Proxy-Server

Der Begriff *Proxy* bedeutet soviel wie „Stellvertreter“ und bezeichnet einen Server, der zwischen den Computer des Benutzers und das Internet geschaltet ist. *Proxy-Server* sind für die Zwischenspeicherung häufig abgerufener Webseiten zuständig und können dadurch den Seitenaufbau beschleunigen.

Rechtsträger

Kirchliche Körperschaften wie Kirchengemeinden, Diakoniestationen und Dekanate werden als *Rechtsträger* bezeichnet. Ein *Rechtsträger* ist Träger von Rechten und Pflichten und kann eine natürliche oder eine juristische Person sein.

Router

Ein *Router* ist ein Gerät, das Datenpakete von einem Netzwerk in ein anderes weiterleitet. Mit einem *Router* kann auf allen Computern eines lokalen Netzwerks der Zugang zum Internet ermöglicht werden.

Hier werden die in dieser Broschüre verwendeten (Fach-)begriffe verständlich erklärt.

Sicherheitsupdates

sind regelmäßig von Microsoft zur Verfügung gestellte Aktualisierungen für die Windows-Betriebssysteme, mit denen Sicherheitslücken geschlossen werden.

SP (Servicepack)

Ein *Servicepack* ist eine Zusammenstellung einzelner Aktualisierungen und Updates für ein Betriebssystem oder Computerprogramm.

SUSE OpenExchange

ist die zentrale Mailserversoftware, die das Senden und Empfangen von E-Mails @ekhn-net.de steuert.

UMTS

(Universal Mobile Telecommunication System) ist das Mobilfunksystem der sogenannten "dritten Generation", das aufgrund hoher Übertragungsraten neben Sprachkommunikation auch Multimedia- und Internet-Anwendungen erlaubt. *UMTS* ermöglicht Übertragungsraten bis 384 kbit/s.

Voice-Over-IP

Voice-Over-IP ermöglicht das kostengünstige Telefonieren über das Internet. Bei *Voice-Over-IP* wird das Sprachsignal in Datenpakete umgesetzt und über das Internet Protokoll (IP) gesendet.

VPN

VPN ist die Abkürzung für „*Virtuelles privates Netzwerk*“. Beim *VPN* wird über das öffentliche Internet ein gesicherter und verschlüsselter Datentunnel zwischen Ihrem PC und der Kirchenverwaltung bzw. dem Rechenzentrum aufgebaut.

Webmail

Als *Webmail* werden Dienste im Internet bezeichnet, die die Verwaltung von E-Mails mit einem Webbrowser ermöglichen. Ein spezielles E-Mail-Programm wie z.B. Outlook, wird dabei nicht benötigt.

Winkita

Mit *Winkita* erfolgt in den Regionalverwaltungen die Beitragserhebung und –abrechnung für die angeschlossenen Kindertagesstätten. *Winkita On Web* ist die Web-basierte Weiterentwicklung von *Winkita*, die den Kindertagesstätten den Zugriff auf die eigenen Stammdaten ermöglichen soll.

WLAN

ist die Abkürzung für *Wireless Local Area Network* und bezeichnet ein Netzwerk, das nicht auf Kabel als Verbindungselemente angewiesen ist, da die Datenübermittlung per Funk erfolgt.

Zertifikat

Ein *Zertifikat* ist ein elektronischer Ausweis, der die Identität einer Person oder eines Zugangscodes bestätigt.