B e r i c h t
des Landeskirchenamtes
betr. IT-Konzept 2020 der hannoverschen Landeskirche

Hannover, 10. November 2017

In der Anlage übersenden wir den von der Landessynode erbetenen Bericht des Landeskirchenamtes betr. IT-Konzept 2020 der hannoverschen Landeskirche.

Das Landeskirchenamt
Dr. Springer

Anlage

I.
Auftrag und Ausgangslage

Die 24. Landessynode hatte während ihrer IV. Tagung in der 13. Sitzung am 7. Mai 2009 im Zusammenhang mit der Verhandlung über den Tätigkeitsbericht des Landessynodalausschusses (Aktenstück Nr. 3 D, Ziff. 18) auf Antrag des Synodalen Dr. Hasselhorn folgenden Beschluss gefasst:

> *"Das Landeskirchenamt wird gebeten, in Abstimmung mit dem Fachausschuss der Kirchenkreisämter, alsbald ein 'IT-Konzept 2020' vorzulegen, welches beschreibt, welche IT-Ausstattung (Hardware und Software) im Jahr 2020*
> - *im Landeskirchenamt und in den zentralen Einrichtungen der hannoverschen Landeskirche,*
> - *in den Kirchenämtern und*
> - *in den Kirchengemeinden*
>
> *vorgehalten werden soll und welche Zugangs- und Nutzungsmöglichkeiten im Jahr 2020 für Ehrenamtliche bestehen sollen."*

(Beschlusssammlung der IV. Tagung der 24. Landessynode Nr. 2.9)

Daraufhin hatte das Landeskirchenamt mit dem Aktenstück Nr. 104 der 24. Landessynode in ihrer X. Tagung am 16. Juni 2012 einen ersten Bericht zum IT-Konzept in der Evangelisch-lutherischen Landeskirche Hannovers vorgelegt, in dem auch Eckpunkte für eine IT-Strategie niedergelegt wurden. Trotz (im Vergleich zu anderen Gliedkirchen) einem geschlossenen und sicheren Kirchennetz zeigte sich innerhalb der Landeskirche ein sehr heterogenes Bild in der Verfügbarkeit und im Support von IT.

Basierend auf diesem Eckpunktepapier wurden in der folgenden Zeit neben regelmäßigen Beratungen im Schwerpunkteausschuss die Strukturen der IT in der Landeskirche fortentwickelt, u.a.:

- Verhandlung von Rahmenverträgen für kirchliche Kernanwendungen
- Bezuschussung von Kirchennetzzugängen für Meldewesennutzende in den Kirchengemeinden
- Entwicklung und Aufbau eines neuen Intranet für Haupt- und Ehrenamtliche
- Mitberatung bei den Themen Datenschutz und IT-Sicherheit auf Ebene der Evangelischen Kirche in Deuschland
- Unterstützung, zentraler Betrieb und zentrale Finanzierung von Kernanwendungen
- Aufbau einer neuen zentralen Authentifizierungslösung
- Erste Umsetzungen von IT-Sicherheitsregelungen (Meldewesenzugänge)
- Konzeption und Aufbau einer neuen zentralen E-Mail-Infrastruktur

Sich ändernde rechtliche Anforderungen, eine immer höher werdende Komplexität im Betrieb von IT sowie Kostensteigerungen führen dazu, dass die bisherige technische und organisatorische IT-Struktur in der Landeskirche grundlegend zu überdenken ist, um diese an die aktuellen Bedürfnisse der Nutzer und Nutzerinnen einerseits und an die rechtlichen Rahmenbedingungen andererseits anzupassen. Neben einer laufenden Beratung im IT-Ausschuss der Kirchenämter für ein IT-Konzept erfolgten weitere Beratungen im Landessynodalausschuss am 23. Juni 2016 sowie eine durch den Schwerpunkteausschuss einberufene Tagung im Januar 2017. Die Ergebnisse dieser Tagung (insbesondere die Themen "Einheitliche E-Mail", "Rolle der Kirchenämter", "Ausstattung mit Endgeräten") wurden der 25. Landessynode im Mai 2017 mit dem Aktenstück Nr. 80 als Zwischenbericht vorgestellt.

Neben der Erprobung technischer Lösungen, Preisverhandlungen mit Anbietern und Lizenzgebern haben im Jahr 2017 folgende Gremienberatungen zum IT-Konzept stattgefunden:

- IT-Ausschuss der Kirchenämter zur Frage der Rolle der Verwaltungen im Bereich der IT,
- Beratungen im Öffentlichkeitsausschuss der Landessynode zur Frage einer einheitlichen E-Mail-Adresse,
- Beratungen im Ausschuss für kirchliche Mitarbeit der Landessynode zur Frage einer Compliance-Regelung.

II.
Zielsetzung eines IT-Konzeptes und Rahmenbedingungen

Basierend auf dem Aktenstück Nr. 104 der 24. Landessynode aus dem Jahr 2012 wird mit dem vorliegenden Papier das IT-Konzept der hannoverschen Landeskirche fortgeschrieben und den veränderten Rahmenbedingungen angepasst. Es soll eine optimale Arbeitsunterstützung der Nutzer und Nutzerinnen erreicht werden, unter Beachtung der Rahmenbedingungen Datenschutz, IT-Sicherheit und Wirtschaftlichkeit.

Das IT-Konzept soll die Grundlage für eine gute elektronische Kommunikation sein und muss aufgrund der sich stetig entwickelnden Technik auch zukünftig regelmäßig fortgeschrieben werden.

Mit dem IT-Konzept soll eine stärkere Strukturierung und Standardisierung der IT in der Landeskirche einhergehen, als dies bisher der Fall war. Dies erstreckt sich auf die Bereiche:

- Standardisierung von Infrastruktur und Fachanwendungen
- einheitliche Datenschutzstandards
- einheitliche IT-Sicherheitsstandards
- einheitliche Lizensierung
- klare Kostenverteilung

Eine Strukturierung bedingt auch organisatorische Abgrenzungen:

- Das IT-Konzept umfasst alle Körperschaften und unselbständigen Einrichtungen in der Evangelisch-lutherischen Landeskirche Hannovers.
- Eine Aufnahme anderer Einrichtungen (GmbH, e.V., etc.) in die IT-Struktur ist (u.a. wegen Lizenzbedingungen, IT-Sicherheit, Datenschutz, Umsatzsteuer) nicht vorgesehen. Sofern diese Einrichtungen in der Vergangenheit mitversorgt wurden, ist auf eine Trennung hinzuarbeiten.

III.
Vorarbeiten für ein IT-Konzept

Für eine neue IT-Konzeption wurden durch das Landeskirchenamt auf Basis der Ergebnisse der Tagung im Januar 2017 (s. Aktenstück Nr. 80) folgende Themen fortentwickelt, gemeinsam mit externen Beratern geprüft und - soweit möglich - ersten Praxistests unterzogen:

- Prüfung der Strukturen und Regelungen in anderen Landeskirchen
- Prüfung der Ausstattung mit Endgeräten inclusive der Anforderungsaufnahme im Pfarramt
- Bring Your Own Device Strategien
- Diskussion von Pflicht- und Wahlaufgaben für Kirchenämter im Bereich der IT
- Prüfung einer veränderten Netzkonzeption mit einheitlichen Sicherheitsstandards für bestimmte Daten
- Sicherheitsbetrachtung von Mobilgeräten
- Möglichkeiten der E-Mail-Verschlüsselung
- Lizenzverhandlungen und Kostenschätzungen

Festzustellen ist weiterhin, dass für den Einsatz von IT in der hannoverschen Landeskirche bisher wenig klare rechtliche Grundlagen vorliegen. Die vorhandenen Regelungen sind wenig kodifiziert und über die Jahre gewachsen, was regelmäßig zu Unklarheiten führt.

IV.
Inhalt und Regelungen

IT-Konzept und technische Dokumentation

Neben der Vorlage eines IT-Konzeptes 2020 (es ist in der Anlage zum Aktenstück abgedruckt) hat das Landeskirchenamt eine technische Dokumentation der bisherigen Standards entwickelt, die künftig fortzuschreiben ist. Folgende sieben Themen des IT-Konzeptes sind zentral für die weiteren Überlegungen:

1. Kirchennetz - Informationsverbund

   Das sichere Kirchennetz in seiner jetzigen Form wird überarbeitet und zu einem definierten Informationsverbund umgestaltet. In diesem Informationsverbund gelten einheitliche Standards, Benutzer und Geräte sind in einem zentralen Nutzerverzeichnis gepflegt. Ein IT-Sicherheitskonzept sowie Umsetzung von Datenschutzstandards werden zentral etabliert. Aus dieser neuen Netzstruktur werden Übergabepunkte an nicht gemanagte Geräte oder andere Umgebungen definiert. Die bestehenden Umgebungen der Kirchenämter und anderer größerer Einrichtungen werden sukzessive in diese neue Umgebung integriert. Ein zentraler Aspekt der neuen Struktur soll eine Portallösung sein, an der man sich sowohl mit dienstlichen wie auch privaten Geräten anmelden kann, um verschiedene zentrale Anwendungen der Landeskirche zu nutzen. Dies ist dann auch der Zugangspunkt für kleine Einrichtungen und Kirchengemeinden mit Einzelplatzanbindungen.

2. Infrastruktur – Virtueller Arbeitsplatz

   Über eine zentrale Portallösung wird die Möglichkeit eines virtuellen Arbeitsplatzes bereitgestellt. Nutzer und Nutzerinnen können sich mit einem beliebigen Endgerät an einer dienstlichen Umgebung anmelden und haben Zugriff auf einen komplett virtuell bereitgestellten dienstlichen Computer (PC) sowie dienstliche Daten. Dies erleichtert die Zusammenarbeit bei Arbeitsplatzwechseln und verteilten Standorten und unterstützt die Forderung, private Endgeräte einsetzen zu wollen. Die dienstliche virtuelle Umgebung wird richtig lizensiert und die genutzten Daten werden gesichert. Voraussetzung hierbei ist eine vorhandene und ausreichende Datenverbindung.

3. Einheitliche E-Mail

   Mit der Bereitstellung eines zentralen E-Mail- und Groupwaresystems (Adressbuch, Kalender) für alle hauptberuflich Mitarbeitenden soll die Kommunikation in der Landeskirche verbessert und Regelungen des Datenschutzes eingehalten werden. Durch eine einheitliche E-Mail-Endung wird auch die Landeskirche als Institution in der Kommunikation sichtbarer. In Zusammenarbeit mit dem Kommunikationskonzept ist eine Veränderung der einheitlichen E-Mail-Endung von "@evlka.de" in eine neue E-Mail-Endung angedacht. Das Landeskirchenamt schlägt als neue Endung "@evlkh.de" vor.

4. Einbindung ehrenamtlicher Gremienvertreter

   Die Einbindung Ehrenamtlicher in zentrale IT-Strukturen wird im Konzept mitbedacht, allerdings sind Kosten und Organisation bei einer Vielzahl von Personen, die sich in ihrer Gremienzusammensetzung auch ändern, sorgfältig zu planen. Eine Überlegung ist, im Rahmen der Kirchenvorstandswahl jedem neuen Kirchenvorstand eine Möglichkeit zu eröffnen, ein dienstliches E-Mail-Postfach sowie Zugriff auf ein Portal für Gremienvertreter zu erhalten.

5. Ausstattung mit Endgeräten

   Sowohl die Diskussion mit anderen Landeskirchen als auch die technischen Vorüberlegungen haben gezeigt, dass bei der Frage der Endgeräteausstattung weniger die Geräte selbst eine Frage sind, als vielmehr die technische Infrastruktur, um so eine Anbindung verschiedenster Geräte zu ermöglichen. Für die Ausstattung mit Endgeräten wird die Landeskirche:
   - künftig Empfehlungen für Neuanschaffungen herausgeben,
   - ein Angebot für voll gemanagte Endgeräte entwickeln,
   - eine Möglichkeit der Anbindung von privaten und nicht gemanagten dienstlichen Geräten entwickeln.

   Diese Dreiteilung basiert auf Erfahrungen anderer Organisationen, die zeigen, dass:
   - ein flächendeckendes Ausrollen von Geräten, die vom Nutzenden nicht verändert werden können, nicht überall auf Akzeptanz stößt. Die in diesem Verfahren hohe Sicherheit wird umgangen, indem mit anderen Geräten vor Ort gearbeitet wird,
   - eine Nutzung von Geräten, die die Nutzenden administrieren und ggf. auch selbst beschaffen können, i.d.R. nicht den Sicherheits- und Datenschutzvorschriften genügen und Lizenzverstöße wahrscheinlich sind,
   - ein Mischbetrieb von Regelungen zu unklaren Zuständigkeiten und damit auch zu Sicherheitsrisiken führt.

Eine Entscheidung über die Art der Beschaffung und Bereitstellung sollte vom jeweiligen Anstellungsträger erfolgen.

Um einen endgeräteunabhängigen Zugriff zu ermöglichen, sollen im IT-Konzept künftig zumindest die zentralen Anwendungen, die über einen hohen Schutzbedarf verfügen, über ein einheitliches Portal zur Verfügung gestellt werden, das grundsätzlich von überall erreichbar ist. Auf Basis von personalisierten Zugangsberechtigungen einerseits und Prüfmechanismen, mit welchem Gerät und mit welcher Sicherheit zugegriffen wird, können den Nutzenden dann entsprechend Zugriffe auf Programme und Daten gewährt werden. Das lässt dann sowohl die Anbindung vollgemanagter Endgeräte zu, bei denen die Anwender und Anwenderinnen sich nicht um Sicherheitsfragen kümmern müssen, als auch den Zugriff auf das Portal mit privaten Endgeräten. Auch ohne "sicheres" Endgerät soll dann ein Arbeiten auf dem "virtuellen Arbeitsplatz" möglich sein. Diese Lösung unterstützt weiterhin die immer mobiler werdenden Arbeitsplätze, bei denen oft auf die gleichen Informationen von unterschiedlichen Standorten zugegriffen werden muss.

6. Organisatorische Verantwortung – Rolle der Kirchenämter

Nach den Vorüberlegungen, auch gemeinsam mit den Fachverantwortlichen aus den Verwaltungen, müssen die Kirchenämter eine tragende Rolle in der Versorgung von Kirchengemeinden mit IT spielen. Nur in den Verwaltungen gibt es verlässliche Informationen über die Neueinstellungen und das Ausscheiden von Mitarbeitenden und Gremienmitgliedern, sodass die Steuerung der IT in den Kirchenämtern erfolgen muss. Dies beinhaltet mindestens die Verwaltung und Rechtezuordnung der Nutzenden. Insofern sollte diese IT-Aufgabe für die Ämter als Pflicht geregelt werden, die sich in der Ausführung dann auch externer Dienstleister bedienen können.

7. Rechtlicher Rahmen

Über das Konzept hinaus bedarf es jedoch – vergleichbar zu anderen Gliedkirchen der Evangelischen Kirche in Deutschland – eines rechtlichen Rahmens zur IT-Nutzung in der hannoverschen Landeskirche. Damit würde eine Grundlage für alle weiteren künftigen Überlegungen gebildet, ein klarer Rahmen geschaffen und die Bezüge zu weiteren geltenden Rechtsvorschriften (Datenschutz, IT-Sicherheit) herstellt.

Ein rechtlicher Rahmen könnte folgende Themen regeln:

- Festlegung und Standardisierung der wichtigsten Anwendungen (Meldewesen, Finanzwesen, Personalabrechnung, Kommunikation). Dies folgt den Überlegungen der Landessynode, Standards in der IT-Nutzung zu fördern.

- Die Vorgabe einer einheitlichen E-Mail-Lösung als Grundlage, um ein einheitliches Kommunikationskonzept zu entwickeln.
- Abgrenzung von dienstlichen und privaten Umgebungen mit entsprechenden Nutzungsvereinbarungen
- Organisatorische Verantwortung auf den verschiedenen Ebenen der Landeskirche

Für die Frage der Compliance wäre mit einem Rechtsrahmen und einer einheitlichen Dienstvereinbarung eine Grundlage geschaffen, alle Mitarbeitenden auf die Einhaltung der Regelungen im Zusammenhang mit der IT-Nutzung zu verpflichten. Unabhängig hiervon sind regelmäßige Informationen aller Mitarbeitenden zum Thema IT-Sicherheit und Umgang mit dienstlichen Daten notwendig.

V.
Nächste Schritte, Kosten

Das IT-Konzept 2020 wird mit den Ausschüssen der Landessynode und den Vertretungen der Kirchenämter ausführlich zu beraten sein.

Die nächsten Schritte in der Fortentwicklung des IT-Konzeptes sind die Entwicklung von Feinkonzeptionen, die Erarbeitung rechtlicher Regelungen sowie die weitere Umsetzung der Anbindung von Verwaltungen an die zentrale Infrastruktur. Im Detail sind folgende Schritte für die weitere Bearbeitung des IT-Konzeptes geplant:

- Anbindung der Kirchenämter an einheitliche Infrastruktur (laufend)
- Feinplanung der Konzeption (bis Mai 2018)
- Entwurf für rechtliche Regelungen (bis Mai 2018)
- Umsetzung zentrale E-Mail für alle (laufend bis 2022)
- Anbindung der neuen Kirchenvorstände (Mitte 2018)
- Konzeption und Umsetzung Zentrales Portal (bis Ende 2018)
- Kostenschätzung für weitere Ausbaustufen
- Angebot für standardisierte Endgeräte (ab Januar 2019), und/oder alternativ Zuschuss zu Beschaffung vor Ort

Die vorgesehene Zeitplanung ist ambitioniert und im Verlauf des Projektes zu verifizieren oder anzupassen. Die für Konzeption, Umbau von Infrastruktur sowie Aufbau neuer Lösungen im IT-Konzept grob geschätzten einmaligen Kosten in Höhe von 2,65 Mio. Euro können weitgehend über vorhandene Haushaltsmittel finanziert werden. Es ist zum einen

geplant, im Jahr 2017 eine entsprechende Rückstellung noch nicht verausgabter Mittel zu bilden, zum anderen sind Haushaltsmittel für das Jahr 2018 eingeplant, die nach Vorliegen eines Detailkonzeptes vom Landessynodalausschuss freigegeben werden können.

Eine vollständige Finanzierung aller anfallenden IT-Kosten zentral durch die Landeskirche ist wenig effizient, da ansonsten eine umfängliche Vollausstattung finanziert wird, der wenig Nutzung gegenübersteht. Insofern müssen auch nutzer- oder nutzungsabhängige Kosten in der Landeskirche verteilt werden, ohne den Anreiz einer zentralen Finanzierung für eine Standardisierung zu vernachlässigen. Im Rahmen des zu erstellenden Feinkonzeptes ist daher zu bedenken, welche Basisfinanzierungen durch die Landeskirche erfolgen sollten und welche gut verteilbaren weiteren Kosten sinnvoll verteilt werden können. Für die Ausstattung mit Endgeräten könnte beispielsweise der jeweilige Anstellungsträger sorgen.

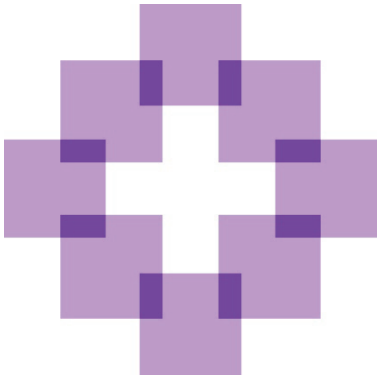
Die mit dem neuen IT-Konzept anfallenden laufenden Kosten werden, sofern es zwischen den Ebenen der Landeskirche finanzielle Umverteilungen zu bisherigen Lösungen gibt oder die neu entstehenden Kosten nicht durch Einsparungen kompensiert werden können, in der Haushaltsplanung für die Jahre 2019 und 2020 zu berücksichtigen sein. Insofern sind die Detailplanungen bis Mitte 2018 abzuschließen.

VI.
Fazit

Das Vorhalten einer sicheren und nutzerorientierten IT wird in Zukunft für die kirchliche Arbeit immer wichtiger. Für eine steuerbare IT-Infrastruktur ist eine höhere Standardisierung als bisher notwendig. Mit dem vorliegenden IT-Konzept beschreitet die hannoversche Landeskirche einen Weg in eine stärkere Vereinheitlichung ohne jedoch die individuellen Bedürfnisse in der Fläche der Körperschaften außer Acht zu lassen.

Anlage

Anlage



IT-Konzept 2020

der

Evangelisch-lutherischen Landeskirche Hannovers

Herausgeber

Evangelisch-lutherische Landeskirche Hannover
Das Landeskirchenamt
Referat 64 (IT und Controlling)
Goethestrasse 29
30169 Hannover

Dokumentenverantwortung

Das IT-Konzept ist vom Referat 64 des Landeskirchenamtes in Hannover erarbeitet worden.

Name	Position	Telefon	E-Mail
Stefan Schierding	Leiter IT-Strategie	0511-1241176	Stefan.Schierding@evlka.de

Versionsübersicht

Das IT-Konzept ist in der hier abgebildeten Version gültig und ersetzt damit alle älteren Versionsstände.

Version	Datum	Verfasser	Beschreibung
Alpha 1.0	29.09.2017	Schierding	Entwurf
1.1	03.10.2017	Spier	Entwurf
1.2	12.10.2017	Spier/Schierding	Entwurf
1.3.	13.10.2017	Dr. Krämer / Spier /Schierding	Finale Version
1.4	02.11.2017	Spier/Schierding	Änderungswünsche aus dem Kolleg eingearbeitet

Inhalt

1. Ausgangslage

Die Evangelisch-lutherische Landeskirche Hannovers ist eine Flächenorganisation, die sich über einen Großteil des Bundeslandes Niedersachsens erstreckt. Neben dem Landeskirchenamt mit ca. 250 Arbeitsplätzen gibt es ca. 25 Verwaltungsämter mit im Durchschnitt 20-50 Arbeitsplätzen, die Verwaltungsaufgaben für die jeweiligen Kirchengemeinden in ihrem Einzugsbereich erfüllen. Zu diesen ca. 1300 Kirchengemeinden (Standorte mit in der Regel 1-2 Arbeitsplätzen) kommen noch diverse diakonische Einrichtungen, Jugendwerke, Seelsorgeeinrichtungen, Tagungsstätten usw. hinzu, die elektronisch Daten austauschen. Für die aktuellen vorhandenen IT-Standards gibt es eine technische Dokumentation, die laufend fortgeschrieben wird.

1.1 Sicheres Kirchennetz

Der Datenaustausch zwischen den Gemeinden, Einrichtungen, Kirchenämtern, dem Rechenzentrum und dem Internet findet grundsätzlich über das sogenannte „sichere Kirchennetz“ statt. Hierbei handelt es sich um ein Netz für den dienstlichen Gebrauch, über das dienstliche Informationen ausgetauscht werden. Jede Einrichtung, die dienstliche Informationen nutzen möchte, benötigt einen Anschluss an das Kirchennetz. Die Kommunikation zwischen allen Dienststellen erfolgt verschlüsselt, d.h. ist vor dem Zugriff Dritter aus dem Internet geschützt. Damit erfolgt eine Abgrenzung des Kirchennetzes von anderen Netzen sowie dem Internet und somit die Schaffung eines Virtuellen Privaten Netzwerks (VPN).

1.1.1 Zentralisierte Sicherheitsstrukturen

Dieses Kirchennetz weist eine sternförmige Netztopologie auf. Im Zentrum dieser Stern-Struktur befinden sich zentrale Sicherheitssysteme, die den gesamten Netzwerkverkehr regeln. Die Kommunikationsverbindungen zwischen den Standorten werden grundsätzlich über dieses zentrale Sicherheitssystem geführt.

1.1.2 Zentraler Internetzugang

Der Zugriff auf das Internet von einem dienstlichen Arbeitsplatz aus erfolgt transparent über einen zentralen geschützten Internet-Anschluss. Dieser Anschluss wird über den zentralen Infrastruktur-Dienstleister (Comramo AG) im Rechenzentrum in Hannover bereitgestellt. Dieser übernimmt dabei auch die Namensauflösung der Adressen, das Routing der Anfragen und die ordnungsgemäße Übersetzung der internen Netzadressen in öffentliche Adressen.

1.1.3 Standardisierte Einzel- und Mehrplatzeinwahl

Das Kirchennetz bietet die Möglichkeit, ganze Standorte (Mehrplatz) oder nur einzelne Anwender (Einzelplatz) über einen sicheren verschlüsselten Zugriff an das zentrale Rechenzentrum anzubinden. Mehrplatzstandorte (große und kleine Netze) werden in der Regel über Hardware-Lösungen angebunden. Einzelplätze werden über Software Lösungen angebunden. Mobile Endgeräte wählen sich über spezielle zur Verfügung gestellt Zugangspunkte ein. Die eingesetzten Lösungen sind hochstandardisiert und werden den Dienststellen vom Infrastrukturdienstleister der Landeskirche als Produkte direkt angeboten.

1.1.4 Zentrales Hosting

Für verschiedene Fachverfahren werden landeskirchenweit standardisierte Anwendungen im zentralen Rechenzentrum des Infrastrukturdienstleisters betrieben. Der zentrale Betrieb fördert die Wirtschaftlichkeit des Einsatzes von IT und verbessert die Konformität der Informationssicherheit.

1.1.5 Schutzklassen für Informationen

Grundsätzlich kann eine Einteilung der Informationen in drei Schutzklassen erfolgen: personenbezogen, dienstlich schützenswert und öffentlich. Der dienstlich schützenswerte Bereich beinhaltet dienstliche Informationen, die nicht für die Öffentlichkeit bestimmt sind, und bildet die mittlere Schicht. Diese ist auch aus dem Internet zugänglich, wird aber in der Regel durch Zugriffsbeschränkungen, d.h. Logins und eine Transportverschlüsselung geschützt. Der Bereich „personenbezogen“ enthält besonders sensible personenbezogene Daten, wie z.B. kirchliche Melde-, Personal-, Spenden- und Patientendaten und darf nur innerhalb des VPNs erreichbar sein. Der öffentliche Bereich ist für alle, d.h. auch aus dem Internet direkt zugänglich und enthält nur öffentliche Informationen.

1.2 Kirchliche Dienststellen

1.2.1 Hard- und Softwarestand

Ein einheitlich festgeschriebener Hardware- und Software-Standard ist aktuell innerhalb der Landeskirche nicht vorhanden. Die Ausstattung mit IT wird anhand der örtlichen Haushaltsmittel entschieden. In Ermangelung zentraler Mindestvorgaben sowie einer Budgetierung im Rahmen einer Gesamtzuweisung von Haushaltsmitteln gibt es hier ganz unterschiedliche Ausprägungen hinsichtlich der Modernität der IT-Ausstattung. So sind z.B. vielfach noch PC Altsysteme mit im Einsatz, für die es seit Jahren keine

Sicherheitsaktualisierungen mehr gibt. So stellen diese Arbeitsplätze ein nicht kalkulierbares Sicherheitsrisiko dar. Teilweise wird dienstliche Hard- und Software mit privater kombiniert und ergänzt und mit Unverständnis reagiert, wenn der Support dieser Landschaft zu Problemen und deutlichem Mehraufwand führt.

Ähnlich unkoordiniert wie die Hard- und Software-Ausstattung verläuft in der Regel auch der Umgang mit Lizenzen. Die Anwenderinnen und Anwender sind hier überfordert mit komplexen Lizenzbedingungen und mischen Lizenzen aus dem Kaufhaus, nur für den Privatgebrauch gedachten Lizenzen und Lizenzen aus Rahmenverträgen, ohne zu hinterfragen, ob diese Nutzungsberechtigungen überhaupt in ihrem Einsatzbereich und in dieser Kombination Gültigkeit besitzen.

1.2.2 Betreuung

Die Betreuung der Arbeitsplätze ist uneinheitlich geregelt. Für die standardisierten Netzprodukte und die zentral bereitgestellten Produkte stellt die Landeskirche über den zentralen Infrastrukturdienstleister eine Hotline zur Verfügung. Die Betreuung der Arbeitsplätze vor Ort ist von den jeweiligen Einrichtungen individuell geregelt.

Jedes Kirchenamt hat einen oder mehrere IT-Zuständige, genannt Systemverwalterinnen und Systemverwalter, die in der Einrichtung entweder mit einer ganzen Stelle oder nur mit einer Teilstelle die IT-relevanten Betreuungsaufgaben vor Ort wahrnehmen. Betreuungsumfang und Intensität sind demzufolge in jedem Kirchenkreisamt in unterschiedlicher Ausprägung individuell geregelt. Die Systemverwalter bilden auch die Schnittstelle zum zentralen Infrastrukturdienstleister sowie weiteren lokalen Dienstleistern bei Problemen und Fragestellungen.

Jedes Kirchenkreisamt entscheidet individuell und autonom, ob es bestimmte IT-relevante Betreuungsaufgaben ganz oder auch nur teilweise an externe Servicepartner vergeben möchte, und beauftragt dann selbstständig die Fremdfirma. Das können Einzelaufträge sein oder auch längerfristige Supportverträge. In der Regel bilden auch hier die Systemverwalter die Schnittstelle zum Servicepartner. In Ermangelung zentraler Vorgaben kann die Beratung der Dienstleister auch dazu führen, dass in den Dienststellen Lösungen weit ab von vermeintlichen Standards etabliert werden.

1.2.3 Schatten-IT

Das bisherige Konzept unterstreicht den dienstlichen Charakter der Daten und auch der Arbeitsplätze. Anforderungen des Datenschutzes und der Datensicherheit führen zu einem restriktiven Betrieb von Arbeitsplätzen im Kirchennetz, der keine Flexibilität zulässt. Ausnahmen sind nicht umsetzbar. Die technischen Sicherheitslösungen sind in der Regel nicht sehr benutzerfreundlich und vielfach das genaue Gegenteil dessen, was

Anwenderinnen und Anwender aus dem privaten Umfeld gewohnt sind. In Konsequenz bauen sich findige Anwender ihre eigene individuelle Infrastruktur auf, die sie dann für dienstliche Zwecke nutzen, wobei Aspekte der Datensicherheit und des Datenschutzes vielfach vernachlässigt werden. Diese Entwicklung ist mit einem einheitlichen IT-Konzept für die gesamte Landeskirche nicht vereinbar. Dieser Fehlentwicklung kann man rechtlich durch entsprechende Verordnungen entgegenwirken. In gleichen Zug muss jedoch geprüft werden, ob eine bessere Balance zwischen Bedienbarkeit und Sicherheit hergestellt werden kann.

1.3 Aufgabe des IT Konzeptes

Aus dem aktuellen Stand der IT Infrastruktur in der Landeskirche, der ein inhomogenes Bild mit teilweise teuren Insellösungen sowie eine hohe dezentrale Eigenverantwortung darstellt, ergibt sich die Forderung, eine gesamtkirchliche Standardisierung der IT voranzutreiben. Die Neustrukturierung und personelle Aufstockung des IT-Referates im Landeskirchenamt ermöglicht nun eine Umsetzung dieser Forderung.

Im Rahmen einer Gesamtstrategie werden allgemeine strategische Ziele und Handlungsfelder definiert. Daraus ergeben sich neue Anforderungen an die Anbindung der kirchlichen Dienststellen an das sichere Kirchennetz, die in diesem Dokument grob beschrieben werden.

2. Eckpunkte des IT-Konzeptes 2020

2.1 Strategische Ziele

Vorrangiges Ziel ist es, allen Anwendern eine stabile und zuverlässige IT-Umgebung zur Verfügung zu stellen, die ihre Arbeit optimal unterstützt. Noch nicht angebundene dienstliche Arbeitsplätze sollen an diese IT-Umgebung angeschlossen werden. Daraus lassen sich folgende strategische Unterziele bzw. Handlungsfelder ableiten.

2.1.1 Standardisierung

Die Modernisierung der Arbeitsplätze und die Festlegung eines gemeinsamen Hard- und Software-Stand ist notwendig. Dieser Schritt ermöglicht eine homogene und leichter zu administrierende Infrastruktur. Für die Standardisierung ist jeweils ein klar abgegrenzter organisatorischer und technischer Rahmen zu schaffen.

2.1.2 Sicherheit

Aufgrund gesetzlicher Regelungen ist die Schaffung eines landeskirchlichen Sicherheitsniveaus notwendig, das den Anforderungen hinsichtlich Sicherheit und Datenschutz gerecht wird und in einem IT-Sicherheitskonzept dokumentiert wird. Hierzu sind alle eingesetzten Produkte hinsichtlich der verwendeten Daten zu analysieren und in Sicherheitsklassen einzustufen, um auf dieser Basis Sicherheitsmechanismen zu etablieren.

2.1.3 Benutzerfreundlichkeit

Die Verbesserung der Benutzerfreundlichkeit (Usability) der IT-Umgebung ist ein ständiges Kernanliegen. Die IT muss den Anwender in seiner Arbeit unterstützen und darf ihn nicht unnötig behindern. Dabei müssen auch aktuelle Trends berücksichtigt werden. Das erzeugt eine höhere Benutzerakzeptanz und hilft, die Schatten-IT zu reduzieren und zukünftig ganz zu vermeiden.

2.1.4 Zentrale Benutzeranmeldung

Für die Landeskirche soll eine einheitliche Benutzeranmeldung (Authentifizierungsplattform) in Form eines zentralen Verzeichnisdienstes genutzt werden. Diese Plattform soll für sämtliche Anmeldungen (Arbeitsplatz, Zugänge, zentrale Fachanwendungen) innerhalb des sicheren Kirchennetzes genutzt werden, so dass Anwender nach Möglichkeit nur noch einen eindeutigen Benutzernamen und ein einziges Kennwort haben.

2.1.5 Zentralisierung von Anwendungen

Flächendeckend genutzte Fachapplikationen sollen zentralisiert werden. Die Nutzungszugriffe erfolgen auf eine eigene, zentral gehostete und administrierte Serverfarm im Rechenzentrum des zertifizierten landeskirchlichen Dienstleisters.

2.1.6 Einheitliche Kommunikation

Ein zentrales Mailsystems unter einer einheitlichen Maildomain soll die Vereinheitlichung der elektronischen Kommunikation fördern. Zukünftig sollen sich mindestens alle Email-Postfächer der hauptamtlichen Mitarbeitenden der verfassten Kirche im zentralen Mailsystem befinden. Dies ermöglicht laufend die Anpassung von Sicherheits- sowie Verschlüsselungs- und Archivierungsfunktionen. Ebenso werden durch ein einheitliches Adressverzeichnis, Kalenderfunktionalitäten, Terminvereinbarungen bis hin zu einheitlichen Abbindern in Emails die Voraussetzungen für eine gut funktionierende elektronische Kommunikation geschaffen.

2.1.7 Betreuung

Eine gute Betreuungssituation für die IT-Nutzenden kann durch Schaffung klarer Verantwortlichkeiten und Zuständigkeiten bei Administration und Anwenderbetreuung erreicht werden. Hierfür gibt es zwei Voraussetzungen: die klare Trennung von technischen Umgebungen und die Kommunikation von Standards und Anforderungen. Auf dieser Basis kann eine Aufgabenabgrenzung zwischen Hotline, zentraler Betreuung und Vor-Ort-Betreuung erfolgen. Für eine reibungslose Arbeitsplatzbetreuung für Nutzerinnen und Nutzer sollte grundsätzlich die jeweilige zuständige kirchliche Verwaltungsorganisation zuständig sein, die sich weiterer Dienstleister bedienen kann.

2.1.8 Vernetzung

Schaffung einer modernen Netzinfrastruktur, die ein akzeptables Nutzen/Kosten-Verhältnis besitzt. Das beinhaltet stabile, verfügbare Zugänge in ein sicheres Kirchennetz, die genügend Flexibilität hinsichtlich des Anbieters und des Zugangsmediums garantieren.

2.1.9 Compliance

Bestehende Gesetze und Regelungen müssen im Geltungsbereich verbindlich eingehalten werden. Dazu gehören das Datenschutzrecht, das Urheber- und Lizenzrecht sowie Regelungen zur Informationssicherheit.

Zur Vermeidung von Verletzungen des Urheber- und Lizenzrechts muss ein zentralisiertes Lizenzmanagement eingeführt werden. Zur Wahrung der Informationssicherheit muss ein IT-Sicherheitskonzept nach BSI-Standard entwickelt werden. Ebenfalls muss das neue europäische Datenschutzrecht zur Anwendung kommen.

2.1.10 Wirtschaftlichkeit

Da sämtliche Lösungen aus Kirchensteuergeldern finanziert werden, besteht eine besondere Verpflichtung gegenüber unseren Kirchensteuerzahlern, für jedes Verfahren die Wirtschaftlichkeit zu prüfen, ohne die die Nutzungszufriedenheit sowie die Regelungen von Datensicherheit und Datenschutz zu vernachlässigen.

2.2 Abgrenzung und Geltungsbereich

Für das Konzept müssen die Zuständigkeiten und der Geltungsbereiche definiert werden. Hier gelten die folgenden Abgrenzungen.

2.2.1 Verfasste Kirche

Die in diesem Konzept beschriebenen Regelungen gelten für alle Organisationen der verfassten Kirche, die unter der Aufsicht der Ev.-luth. Landeskirche Hannovers stehen. Hierzu zählen neben den kirchlichen Körperschaften insbesondere die landeskirchlichen Verwaltungseinheiten, die Verwaltungseinheiten der Kirchenkreise und Kirchengemeinden sowie alle angeschlossenen unselbständigen Einrichtungen aller Ebenen der Landeskirche. Ausgenommen sind Diakonische- sowie Bildungseinrichtungen in eigener Rechtsträgerschaft und Vereine. Eine nachträgliche Aufnahme anderer Einrichtungen ist nicht vorgesehen. Sofern diese Einrichtungen in der Vergangenheit mitversorgt worden sind, ist unter Berücksichtigung einer Übergangsfrist auf eine Trennung hinzuarbeiten.

2.2.2 Abgrenzung IT-Informationsverbund

Zur technischen und organisatorischen Abgrenzung ist die Definition eines Informationsverbundes notwendig, für den u.a. Dokumentation, Lizensierung, Sicherheit und Zugriffsberechtigungen vereinheitlicht sichergestellt werden müssen. Innerhalb der verfassten Kirche kann es mehrere Informationsverbünde geben. Der Gültigkeitsbereich des betrachteten zentralen Informationsverbundes erstreckt sich auf alle Nutzer, Arbeitsplätze und Serversysteme der Ev.-luth. Landeskirche Hannovers, die im zentralen Nutzerverzeichnis („Active Directory“) verwaltet werden, denn nur diese Systeme können zentral erfasst und administriert werden.

Schnittstellen gibt es zum Rechenzentrum des zentralen Infrastrukturdienstleisters, zum Internet, zu nicht integrierten Dienststellen und Supportdienstleistern.

Körperschaften und Einrichtungen, die ihre Systeme nicht oder nicht komplett in das zentrale Nutzerverzeichnis integrieren wollen, müssen einen eigenen Informationsverbund definieren und somit auch eigenverantwortlich ein eigenes IT-Sicherheitskonzept erstellen.

2.2.3 Ausnahmen

In diesem Konzept werden Telefone und Mobiltelefone nicht näher betrachtet. Die Beschaffung von Hardware und die Schließung entsprechender Nutzungsverträge liegen in der Verantwortung bei den einzelnen Stellen. Für die technische Einbindung von Mobiltelefonen (z.B. Emailempfang) wird eine Mobilgeräterichtlinie erlassen.

3. Benutzerverwaltung und E-Mail

3.1 Zentrale einheitliche Benutzerverwaltung

Ziel

Ziel ist es, alle hauptamtlichen Mitarbeitenden, Server und Arbeitsplätze in der Landeskirche in eine einheitliche landeskirchliche Nutzerverwaltung einzubinden. Dies beinhaltet die Schaffung von Unterstrukturen für die nachgelagerten Kirchenämter und Einrichtungen. Innerhalb der Unterstrukturen sollen beauftragte Administratoren die Anwender und Maschinen in ihrem Zuständigkeitsbereich selbst pflegen.

Zu prüfen ist, inwieweit auch ehrenamtliche Gremienvertreter in der landeskirchlichen Nutzerverwaltung erfasst werden können, um einen validen Adresspool von Ansprechpartnern zu erhalten. Für die pro Nutzendem anfallenden Kosten sind zu budgetieren und ggf. auf die Körperschaften zu verteilen.

Nutzen

Das zentrale Nutzerverzeichnis erleichtert allen Anwenderinnen und Anwendern die Anmeldung am Arbeitsplatz und an zentralen Fachanwendungen. Sie müssen sich nur noch ein persönliches Kennwort merken, um alle angebundenen Anwendungen im Kirchennetz einheitlich zu erreichen. Sogenannte Single-Sign-On Techniken ersparen ihnen eine wiederholte Anmeldung innerhalb ihrer Umgebung. Dieses Verfahren erleichtert außerdem den zuständigen IT-Betreuern die administrative Arbeit, da sie für jeden Nutzer systemweit nur noch einen eindeutigen Zugang für unterschiedliche Anwendungen pflegen müssen. Zusätzlich haben sie damit die Möglichkeit, Updates zentral zu verwalten und organisationsweit gültige Regeln auszurollen.

Außerdem ist eine solche Verwaltung auch Voraussetzung für die Bereitstellung und Nutzung von Lizenzen, die allen hauptamtlichen Nutzerinnen und Nutzern der Landeskirche zur Verfügung gestellt werden.

Umsetzung

In der Startphase erfolgt die Anbindung von dienstlichen Arbeitsplätzen in größeren Einrichtungen. Das IT-Referat des Landeskirchenamtes unterstützt koordinierend und beratend diese Umstellungen.

Um die Pflege dieser Daten zu vereinfachen und die Informationsqualität zu verbessern, wird der Aufbau einer webbasierten Kontoverwaltungsoberfläche notwendig. Der Einsatz notwendiger Werkzeuge wird gerade geprüft. Der Aufbau einer solchen Oberfläche wird bis Ende 2018 angestrebt.

Die erstmalige Migration/Übernahme von Nutzerdaten in das zentrale Verzeichnis erfolgt durch den zentralen Infrastrukturdienstleiter und wird durch die Landeskirche bezuschusst. Ebenfalls bezuschusst werden notwendige zentrale Nutzerlizenzen.

Die Umstellung der Server und Arbeitsplätze vor Ort sowie die weitere Pflege der Nutzerdaten liegt für den gesamten Kirchenkreis im Verantwortungsbereich der Kirchenämter und erfolgt eigenverantwortlich durch die zuständige Systembetreuung. Zur Unterstützung können die Kirchenämter auch externe Dienstleister mit dieser Aufgabe beauftragen.

Angestrebt sind eine komplette Migration des Landeskirchenamtes und aller Kirchenämter bis Ende 2020 und der an das Kirchennetz angebundenen Gemeinden und Einrichtungen bis Ende 2022.

Die Einhaltung dieser Termine setzt allerdings voraus, dass es zeitnah eine verpflichtende Regelung zur Anbindung an diese zentrale Verzeichnisstruktur in Form eines Kirchengesetzes geben wird. Auch muss es eine verpflichtende Regelung geben, die eine Betreuung der Arbeitsplätze nachgelagerter Einrichtungen zur Pflichtaufgabe der Systembetreuung im Kirchenkreisamt macht.

3.2 Standardisierte Email Kommunikation

Ziel

Die Nutzung eines zentralen Exchange Emailservers durch alle hauptamtlichen Mitarbeitenden in der Landeskirche soll als einheitliches Standardkommunikationswerkzeug unter einer einheitlichen Maildomain dienen. Zusätzliche zentrale Sicherheitsfunktionen wie Mailverschlüsselung und Archivierung sollen mit diesem System verknüpft werden. Alte, uneinheitliche Systeme sollten dadurch ersetzt werden. Über eine weitere, alternative Emaildomain wird in Verbindung mit dem Kommunikationskonzept nachgedacht.

Die extern angebundenen und im zentralen Nutzerverzeichnis erfassten ehrenamtlichen Gremienmitglieder könnten ebenfalls über eine cloudbasierte Lösung unter einer einheitlichen kirchlichen Maildomain angebunden werden, um die Kommunikation im Rahmen der Gemeindearbeit zu vereinfachen.

Nutzen

Nutzung eines zentralen Systems zur Etablierung einer einheitlichen Kommunikation und einheitlicher Sicherheitsstandards für alle hauptamtlichen Arbeitsplätze in der Landeskirche. Bereitstellung von Groupware-Funktionen wie gemeinsame Kalender, Ressourcen und Aufgaben. Verbesserung der Verfügbarkeit durch zentrales Hosting im Rechenzentrum. Vereinheitlichte Nutzung durch Outlook, Outlook Web Access und ActiveSync-Clients.

Stärkung der Kommunikation innerhalb der Gemeinden durch Einbindung der ehrenamtlichen Gremienmitglieder.

Umsetzung

Zu Zeit existieren in den nachgelagerten Einrichtungen der Landeskirche lokal betriebene Mailserver. Die Konten sollen im Rahmen der Migration in das zentrale Benutzerverzeichnis ebenfalls auf das zentrale System migriert werden. Erste Verwaltungen sind bereits erfolgreich umgestellt worden. Das IT-Referat des Landeskirchenamtes unterstützt koordinierend und beratend diese Umstellungen.

Die Anlage der Postfächer, die Übernahme der Altdaten, die weitere Pflege der Postfächer sowie die Umstellung der Server und Arbeitsplätze vor Ort müssen für den gesamten Kirchenkreis im Verantwortungsbereich der Kirchenämter liegen und eigenverantwortlich durch die zuständige Systembetreuung erfolgen. Zur Unterstützung können die Kirchenämter auch externe Dienstleister mit dieser Aufgabe beauftragen. Optional kann auch die COMRAMO diese Unterstützungsdienstleistungen für die Kirchenämter erbringen.

Momentan wird die landeskirchliche Maildomäne mit dem Namen „evlka.de“ eingesetzt. Das erfolgt solange, bis eine Entscheidung für eine neue Maildomäne getroffen wird. Das Landeskirchenamt schlägt als neue, einheitliche Endung für alle Mitarbeitenden in der Landeskirche **@evlkh.de** vor.

Eine Verschlüsselungslösung für Emails soll in 2018 evaluiert werden und die Einführung geprüft werden. Anschließend ab 2019 werden die Einsatzmöglichkeiten einer Archivierungslösung und eines gemeinsamen Abbinders evaluiert und deren Einführung geprüft. Eine Projektierung dieser weiteren Schritte wird dann abhängig von den Ergebnissen und den getroffenen Entscheidungen erfolgen.

Angestrebt sind eine komplette Migration des Landeskirchenamtes und aller Kirchenämter bis Ende 2020 und der an das Kirchennetz angebundenen nachgelagerten Gemeinden und Einrichtungen bis Ende 2022.

Die Einhaltung dieser Termine setzt ebenfalls voraus, dass es eine verpflichtende Regelung zur Nutzung des zentralen Mailsystems geben wird. Auch muss es eine verpflichtende Regelung geben, die eine Betreuung der Arbeitsplätze nachgelagerter Einrichtungen zur Pflichtaufgabe der Systembetreuung im Kirchenkreisamt macht.

4. Bereitstellung von zentralen Anwendungen

Ziel

Bereitstellung zentraler Standardanwendungen und Fachverfahren für alle Dienststellen der Landeskirche über eine eigene zentral gehostete und administriertes Nutzerportal Serverfarm im Rechenzentrum unseres zertifizierten Dienstleisters.

Nutzen

Verschiedene Fachverfahren werden von der Landeskirche für alle Dienststellen für eine gemeinsame Nutzung im zentralen Rechenzentrum des beauftragten Infrastruktur-dienstleisters bereitgestellt. Ein zentraler Betrieb zentraler Fachverfahren ist grundsätzlich anzustreben, da ein Hosting in derart professioneller Ausprägung dezentral nur schwer bis überhaupt nicht zu leisten ist.

Umsetzung

Die wichtigsten zentralen Fachverfahren und Applikationen werden bereits als landeskirchliche Standardverfahren zentral im Rechenzentrum gehostet. Dazu gehören das Finanzwesen (Infoma Newsystem), das Personalwesen (KIDICAP P5), Personalmanagement (Unit4 PMS), das Meldewesen (Mewis NT) und Email (Exchange).

Damit definiert die Landeskirche einen zentralen Standard und spricht gleichzeitig eine Empfehlung für diese Produkte aus. Aufgrund der individuellen Anforderungen an die Funktionalität kann in einer Dienststelle der Einsatz einer alternativen Anwendung notwendig werden. Auch hierfür kann die Landeskirche eine Empfehlung aussprechen. Den Betrieb muss dann allerdings die Dienststelle eigenverantwortlich durchführen.

Eine Zentralisierung des Betriebes weiterer Fachanwendungen wird vom Landeskirchenamt geprüft. Bei einer gemeinsamen Entscheidung für einheitliche Anwendungen entscheidet die Landeskirche über eine zentrale Finanzierung.

Die Nutzung dieser zentralen Standardverfahren sollte für alle Dienststellen der Landeskirche verbindlich vorgeschrieben werden. Eine entsprechende Regelung muss verabschiedet werden.

Das IT-Referat des Landeskirchenamtes konzipiert das Nutzerportal und beauftragt die COMRAMO mit dem Aufbau und der zentralen Bereitstellung im geschützten Rechenzentrum. Die Kosten werden zentral getragen.

Angestrebt ist die Bereitstellung eines zentralen Nutzerportals bis Ende 2018.

4.1 Zentrales Nutzerportal mit virtuellem Arbeitsplatz

Die Bereitstellung der zentralen Fachanwendungen mit hohem Schutzbedarf soll zukünftig über ein zentrales Nutzerportal erfolgen. Der Zugriff soll von einem beliebigen Endgerät sowohl aus dem Kirchennetz als auch aus dem Internet möglich sein. Für den Zugriff ein eine Zugriffssoftware notwendig, die eine Verbindung zu dem Portal herstellt und eine Terminalserver-Sitzung öffnet. Die Arbeitsplätze verbinden sich über eine verschlüsselte Verbindung zu diesem Portal. Danach authentifiziert sich die Anwendenden an dem Portal mit Hilfe der im zentralen Nutzerverzeichnis hinterlegten Anmeldedaten und erhalten Zugriff zu einem virtuellen Arbeitsplatz mit den zentral bereitgestellten kirchlichen Anwendungen und Daten. Sämtliche Programme laufen dabei sicher auf den Servern im Kontext der zentralen Terminalserverumgebung. Der lokale PC dient quasi nur noch als Bildschirm mit Tastatur. Damit wird den Anwendern ein virtueller Arbeitsplatz bereitgestellt. Sie haben so die Möglichkeit, sich standortunabhängig mit einem beliebigen Endgerät an einer dienstlichen Umgebung anzumelden und eine virtuell bereitgestellte Arbeitsplatzoberfläche zu nutzen. Dort stehen ihnen neben den dienstlichen Daten und einem Microsoft Office 365 auch ein dienstliches Email-Postfach über Outlook sowie alle zentralen Fachapplikationen, für die eine Berechtigung vorliegt, zur Verfügung.

Die dienstlichen Dokumente werden nicht lokal, sondern in der Kirchennetz-Umgebung auf einem persönlichen Laufwerk gespeichert. Damit kann sichergestellt werden, dass alle zentral gespeicherten Daten mit einem serverseitigen Backup gesichert werden. Bei Bedarf sind noch weitere Laufwerke zur Kooperation zwischen z.B. Gemeinden oder mit dem Kirchenamt vorgesehen. Ein Datenaustausch zwischen lokalen Arbeitsplatzlaufwerken und Netzlaufwerken in der Kirchennetz-Umgebung ist möglich.

Der Datenaustausch von nichtsensiblen Daten mit externen Stellen kann bei Bedarf über ein dienstlich zur Verfügung gestelltes Cloud-Laufwerk realisiert werden.

Wenn sich die Nutzenden von diesem Portal abmelden, dann stehen ihnen die Applikationen und Daten des virtuellen Arbeitsplatzes nicht mehr zur Verfügung, sie können dann lediglich mit den lokal auf dem Arbeitsplatz-Gerät installierten Anwendungen und Daten arbeiten.

Für den Zugriff auf diesen virtuellen Arbeitsplatz ist die Installation eines Terminalserver-Programms und eines geschützten Zugangs zur Portallösung notwendig. Alle weiteren Programme können in dem virtuellen Arbeitsplatz zur Verfügung gestellt werden.

4.2 Perspektivische Weiterentwicklung des zentralen Nutzerportals

Im ersten Schritt muss eine Bereitstellung des zentralen Benutzerportals konzipiert werden. Perspektivisch ist eine Fortentwicklung und Ergänzung um folgende Komponenten sinnvoll.

4.2.1 Erhöhung der Sicherheit durch Zweifaktor-Authentifizierung

Ziel

Ziel der Zweifaktor-Authentisierung ist es, die Sicherheit bei der Anmeldung des Anwenders in potentiell unsicheren Umgebungen zu erhöhen.

Nutzen

Zur Erhöhung der Sicherheit kann für den geschützten Zugriff durch den Einzelnutzer zusätzlich eine Zweifaktor-Authentisierung verwendet werden. Eine verpflichtende Nutzung kann von der Landeskirche in Abhängigkeit des Zugriffs auf bestimmte Daten oder Anwendungen vorgegeben werden. Gerade in potentiell unsicheren Umgebungen, wie z.B. nichtverwalteten oder von mehreren Personen genutzten Rechnern wäre ein Angreifer trotz Kompromittierung der Zugangsdaten des Anwenders durch einen zweiten Faktor nicht in der Lage, auf das Konto des Anwenders zuzugreifen. Zusätzlich zu den vergebenen Zugangsdaten, (Benutzername und Kennwort) benötigt der Anwender noch eine weitere Komponente für den Zugriff, wie ein Zugangstoken.

Umsetzung

Eine Zwei Faktor Authentifizierung muss mit den neuen Einzelplatz-Zugangsprodukten kompatibel sein und muss direkt im Zusammenhang mit diesen Konzepten getestet und eingeführt werden. Eine Erweiterung der Authentifizierung als zusätzliche Option ist zu prüfen.

Eine weitere Projektierung durch das IT-Referat des Landeskirchenamtes findet erst nach der Bereitstellung des Nutzerportals ab 2019 statt.

4.2.2 Erhöhung der Benutzerfreundlichkeit durch ein dienstliches Cloud-Laufwerk

Ziel

Ziel ist es, den unkontrollierten Datenaustausch und den Abfluss dienstlicher Daten über nichtzulässige Speicherorte undefinierter Herkunft zu unterbinden und dafür eine Alternativlösung in einer kontrollierten Umgebung zur Verfügung zu stellen.

Nutzen

Das dienstliche Cloud-Laufwerk soll als dienstliche Lösung eine Alternative zu Dropbox & Co. darstellen und im Rahmen der Anforderungen von Datenschutz und IT-Sicherheit einen kontrollierten Bereich für den Datenaustausch von nichtsensiblen Daten aus der Kirchennetz-Umgebung mit externen Stellen ermöglichen.

Umsetzung

Art und Umfang des Datenaustauschs müssen beschrieben und dem Anwender besonders vor dem Hintergrund der datenschutzrechtlichen Aspekte vorgegeben werden. Dafür muss eine Nutzungsvereinbarung entwickelt werden, die von dem Anwender bei Einrichtung des Laufwerks schriftlich bestätigt werden muss.

Das System muss Clients für Android-, iOS- und Windows Desktopsysteme bereitstellen, die das Synchronisieren und Freigeben von Dateien über eine verschlüsselte Verbindung standortunabhängig ermöglichen.

Das Laufwerk soll eine attraktive Größe und eine hohe Verfügbarkeit haben. Auf einem gemanagten Arbeitsplatz, innerhalb des zentralen Nutzerportals und innerhalb der dienstlichen Umgebung auf dem Mobilgerät muss das Laufwerk dem Anwender uneingeschränkt im Explorer zur Verfügung stehen.

Innerhalb dieser dienstlichen Umgebungen muss der Anwender die Möglichkeit haben, einzelne Dokumente oder ganze Ordner mit anderen Anwendern zu teilen. Dabei soll er selbstständig die Freigaberechte verwalten können.

Zusätzlich soll der Anwender die Möglichkeit haben, nichtsensible Dokumente externen Kommunikationspartnern oder einem externen Arbeitsplatz zum Download zur Verfügung zu stellen. Der Zugriff kann über folgende unterschiedliche Wege muss möglich sein:

- Zugriff durch den Anwender

  Der Anwender kann sich von einem Arbeitsplatz außerhalb des geschützten Kirchennetzes per Explorer oder Weboberfläche mit seinen eigenen Zugangsdaten einloggen und Dokumente hoch- oder runterladen.

- Geschlossener Nutzerbereich

  Der Anwender definiert einen Ordner, den er für diese Funktion nutzen möchte und generiert User-Logins für seine externen Partner, die er ihnen mit einer Einladungsmail zur Verfügung stellt. Die externen Partner können sich dann über einen Webbrowser in diesen Bereich einloggen und die ihnen zur Verfügung gestellten Dokumente herunterladen. Sofern sie die Berechtigung haben, dürfen sie auch Dokumente modifizieren oder neue Dokumente veröffentlichen.

- Anonymer Download

  Der Anwender definiert einen Ordner oder ein Dokument, den er für diese Funktion nutzen möchte und gibt dieses/diesen dann für den anonymen Download frei. Dazu versendet er einen Link per Mail, der Empfänger hat die Möglichkeit, den Link anzuklicken und darüber direkt das Dokument oder den Ordner zu öffnen

Eine Erweiterung des Datenzugriffs durch ein dienstliches Cloud-Laufwerk ist als zusätzliche Option ist zu prüfen.

Eine weitere Projektierung durch das IT-Referat des Landeskirchenamtes findet erst nach der Bereitstellung des Nutzerportals ab 2019 statt.

4.3 Zentrale Webportale

Ziel

Die Bereitstellung der zentralen webfähigen Fachanwendungen mit mittlerem Schutzbedarf soll zukünftig über zentrale Webportale erfolgen. Der Zugriff wird dadurch sehr vereinfacht und soll sowohl von gemanagten Geräten über das Kirchennetz als auch von ungemanagten Arbeitsplätzen möglich sein.

Nutzen

Die Arbeitsplätze verbinden sich mit ihrem Webbrowser über eine SSL-verschlüsselte Verbindung zu diesen Portalen und melden sich mit ihren im zentralen Nutzerverzeichnis hinterlegten Zugangsdaten an. Diese Lösung bietet den Nutzern ein plattformunabhängiges und auch standortunabhängiges Arbeiten.

Auch eine Einbindung in das zentrale Nutzerportal ist möglich, um einen einheitlichen Zugriff über eine einzige Plattform zu haben.

Umsetzung

Erste Webportal-Lösungen sind bereits realisiert, wie z.B. Webmail und Berichtswesen. Ein weiterer Ausbau erfolgt bei Bedarf.

5. Arbeitsplatzausstattung

Im Bereich der Evangelisch-lutherischen Landeskirche Hannovers gibt es eine Vielfalt von Arbeitsplätzen, die ein breites Spektrum von Einsatzmöglichkeiten abdecken. Die wesentlichen Einsatzszenarien sind:

1. Ein stationärer und fest installierter Desktop-Arbeitsplatzrechner in der Verwaltung oder im Gemeindebüro

2. Ein Notebook für Mitarbeiter mit wechselnden Arbeitsplätzen und häufiger Reisetätigkeit

3. Ein mobiles Endgerät für Unterwegs, das das Telefonieren und die Bearbeitung von Korrespondenz ermöglicht

Zukünftig soll die Möglichkeit geboten werden, neben den rein dienstlich gestellten Arbeitsplatzgeräten auch eigenverantwortlich beschaffte Geräte an das Kirchennetz anzubinden. Auch aus diesem Grund ist die Definition von Standards notwendig, um Funktionsfähigkeit, Datenschutz, Informationssicherheit und organisatorische Verantwortung zu gewährleisten.

5.1 Definition eines Arbeitsplatz-Standards

Ziel

Ziel ist es, den hauptamtlichen Mitarbeitern in der Landeskirche einen modernen und zuverlässigen Arbeitsplatz zur Verfügung zu stellen, der sie bei Ihrer täglichen Arbeit unterstützt.

Nutzen

Ein einheitlicher Standard für Arbeitsplätze innerhalb der Landeskirche ermöglicht es, eine homogene und leichter zu administrierende Infrastruktur zu betreiben und Synergieeffekte bei der Beschaffung zu erzielen.

Ein solcher Standard ist die Voraussetzung, vordefinierte Arbeitsplatzpakete in einem Warenkorb anzubieten und über ein Shopsystem bestellbar zu machen. Dienststellen und Einrichtungen, die nicht aus diesem Warenkorb bestellen möchten, dient die Standard-Definition als Empfehlung für eine eigenverantwortliche Beschaffung.

Umsetzung

Das IT-Referat des Landeskirchenamtes entwickelt einen Standard, mit dem sichergestellt wird, dass Arbeitsplatzgeräte optimal an die Strukturen des Kirchennetzes angepasst sind und den Nutzeranforderungen genügen. **Die Definition der Gerätestandards wird bis Mitte 2018 angestrebt.**

Dabei ist zu prüfen, ob eine zentrale Bereitstellung von Geräten erfolgen soll. In diesem Rahmen müssten Geräte bei geeigneten Herstellern ausgewählt werden und Rahmenverträge über die Beschaffung geschlossen werden. Die Geräte könnten im Shopsystem eines geeigneten Herstellers angeboten werden, um einfache und transparente Bestellmöglichkeiten zu schaffen. Ebenso müsste mit den Herstellern und Dienstleistern ein Bestell- und Rollout-Prozess definiert und implementiert werden. Eine ausreichende Garantielaufzeit von 5 Jahren sowie ein schneller Support im Fehlerfall sind ebenfalls essentiell. **Die Bereitstellung einer standardisierten Bestellmöglichkeit wird im Rahmen der Definition der Gerätestandards geprüft und bis Ende 2018 angestrebt.**

5.2 Geräteausstattung

Die Geräteausstattung muss die oben skizzierten Einsatzszenarien unterstützen. Die individuellen Ausstattungsmerkmale müssen mit den Herstellern festgelegt werden. Das IT-Referat der Landeskirche erstellt eine Entscheidungshilfe stellt diese den kirchlichen Stellen zur Verfügung.

5.2.1 Green IT

Beim Kauf der Hardware sollte darauf geachtet werden, dass sie eine Zertifizierung nach TCO besitzt. Ein nach TCO Certified zertifiziertes Gerät erfüllt hohe Nachhaltigkeitsanforderungen während des gesamten Lebenszyklus des Produkts, also in der Herstellungsphase, der Gebrauchsphase und der Entsorgungsphase. Die Einhaltung aller Kriterien wird von einer unabhängigen Prüfstelle verifiziert.

5.2.2 Standard Desktop-Arbeitsplatzrechner

Ein Desktop-Arbeitsplatzrechner ist ein stationäres und fest installiertes Gerät. Es hat die Form eines Desktops oder Minitowers. Die eingebauten Komponenten müssen über ausreichende Leistung verfügen, um ein flüssiges Arbeiten mit Office- und Fachanwendungen zu ermöglichen. Die Anbindung an das Kirchennetz erfolgt kabelgebunden über eine Netzwerkkarte. Die Ausstattung muss einen TFT-Monitor mit Full-HD Auflösung sowie Tastatur und Maus beinhalten.

5.2.3 Notebook

Für Mitarbeiter mit wechselnden Arbeitsplätzen oder mit häufigen Reisetätigkeiten sind Notebooks die erste Wahl. Dieses tragbare Gerät hat eine integrierte Tastatur mit Mauspad sowie ein aufklappbares TFT-Display mit Full-HD Auflösung. Der eingebaute Akku sollte eine Laufzeit von mindestens 8 Stunden unterstützen. Die eingebauten Komponenten müssen über ausreichende Leistung verfügen, um ein flüssiges Arbeiten mit Office- und Fachanwendungen zu ermöglichen. Die Anbindung an das Kirchennetz erfolgt wahlweise kabelgebunden über eine Netzwerkkarte, per WLAN über einen eingebauten WLAN-Adapter oder per UMTS über einen integrierten Mobilfunk-Adapter.

Für den Einsatz im Büro bieten Dockingstationen mit TFT-Monitor, Tastatur und Maus eine ergonomische Ergänzung, so dass ein zusätzlicher Desktop-Arbeitsplatz verzichtbar ist.

5.2.4 Thin-Client

Auf Arbeitsplätzen, wo nur Standard-Applikationen auf einem Terminalserver genutzt werden, macht der Einsatz eines Thin-Clients Sinn. Ein Thin-Client stellt lediglich die Benutzerschnittstelle dar, die Datenverarbeitung erfolgt dabei komplett auf einem zentralen Terminalserver. Auf dem Thin-Client liegen keine Benutzerdaten, sondern nur ein rudimentäres Betriebssystem. Der Vorteil eines Thin-Clients liegt in dem deutlich geringeren Hardware-Bedarf, da nur rudimentäre Softwareinstallationen notwendig sind. So entfällt der Einsatz einer Festplatte und eines Lüfters. Solche Systeme sind außerdem sehr leise und überzeugen durch einen niedrigen Stromverbrauch. Die Konfiguration sowie Software-Updates kann standardisiert über eine zentrale Management-Konsole vorgenommen werden. Neben dem Gerät werden nur noch eine Tastatur und Maus sowie ein TFT-Bildschirm benötigt. Die Anbindung an das Kirchennetz erfolgt kabelgebunden über eine Netzwerkkarte.

5.2.5 Mobile Endgeräte (Smartphones, Tablets)

Mobile Endgeräte sind im weitesten Sinne Smartphones und Tablets. Sie werden für mobile, netzunabhängige Daten-, Sprach- und Bildkommunikation und Navigation eingesetzt. Sie stellen die Verbindung über WLAN oder Mobilfunk-Netze her und kommen in der Regel ohne zusätzliche ein- und Ausgabemedien aus. Die wichtigsten Anwendungsbereiche neben der Telefonie sind das Abrufen von Mails, Kontakten, Terminen, Fotos und Navigationsdaten sowie der Umgang mit Office-Dokumenten. Der Zugriff auf Informationen im Internet wird in der Regel über kleine Applikationen bedient, die sich aus plattformgebundenen App-Stores installieren lassen. Dabei spielen aktuell noch die zwei Betriebssystemplattformen Android und iPhone eine Marktrolle.

Entsprechende Hardware muss sich die kirchliche Stelle eigenverantwortlich beschaffen, ggf. im Rahmen eines Mobilfunkvertrages, der ebenfalls notwendig sein kann.

5.2.6 Drucker / Scanner

Drucker und Scanner stellen die Peripherie zwischen dem auf Papier Gedruckten und der digitalen Welt dar. Der allgemeine Trend zum „papierarmen Büro“ und der zunehmenden digitalisierten Vorgangsbearbeitung verleihen diesen Systemen einen besonderen Stellenwert. Der Einsatz von zentral aufgestellten Multifunktionsgeräten im Netz mit digitaler Kopier-, Druck- und Scanlösung sowie Faxfunktion erscheint an vielen Stellen lohnenswert.

Drucker sollten eine beidseitige Druckoption (fullduplex) als Standard nutzen. Dadurch lässt sich der Papierverbrauch drastisch senken. Bei hohem Druckaufkommen und dem überwiegenden Druck von Geschäftsbriefen ist ein Laserdrucker die bessere Wahl, da die Druckkosten pro Seite geringer sind und das Schriftbild optimaler ist. Bei geringerem Druckvolumen und verstärkter Nutzung von Grafik/Multimedia-Ausdrucken ist ein Tintenstrahldrucker aufgrund der geringeren Anschaffungskosten eine gute Wahl.

Für den Arbeitsalltag im Büro sind sogenannte **Multifunktionsgeräte** eine gute Wahl. Sie vereinen den Drucker, Kopierer, Scanner und Fax in einem Gerät. Solche Multifunktionsgeräte werden in der Regel nicht direkt mit einem Computer verbunden ist, sondern über eine eigene Netzwerkschnittstelle wie eigenständige Server im lokalen Netzwerk angebunden und angesprochen. Das ermöglicht den Zugriff auf diese Geräte von mehreren Arbeitsplätzen aus.

Mit der Einführung von Netzwerkdruckern und Multifunktionsgeräten anstelle von Arbeitsplatzdruckern kann die Zahl der Drucker in einer Dienststelle drastisch reduziert werden, da sich mehrere Nutzer/innen ein zentrales Gerät auf dem Flur teilen, anstatt ihren individuellen Arbeitsplatzdrucker zu nutzen. Auch die Belastung durch Feinstaub wird dadurch gesenkt. In Verbindung mit dem Einsatz von Druckservern wird zudem die Drucker-Administration zentralisiert und somit vereinfacht.

Lokale Arbeitsplatzdrucker werden in der Regel an die USB-Schnittstelle des PC angeschlossen. Ältere Schnittstellen sollten nicht mehr verwendet werden.

5.3 Software

Hinsichtlich der eingesetzten Software gibt es eine Affinität zu den Microsoft- und Microsoft-kompatiblen Produkten. Desktop-Installationen mit Apple OS oder Linux werden im zentralen Informationsverbund der Landeskirche deshalb nicht unterstützt. Eine Anbindung von z.B. Apple-Geräten an die landeskirchliche Infrastruktur wird gleichwohl ermöglicht. Durch diese

Standardisierung wird eine breite Produktunterstützung durch eine Vielzahl von Herstellern und eine breite Auswahl von Support-Dienstleistern für die Betreuung der Arbeitsplätze gegeben.

5.3.1 Desktop-Betriebssysteme

Als Desktop Betriebssystem wird Microsoft Windows Professional oder Enterprise in der 64 Bit Version eingesetzt. Ältere Versionen sollten allein aus Sicherheitsgründen und mit Hinblick auf den Update-Support nicht mehr betrieben werden. Neugeräte sollten grundsätzlich gleich mit einer entsprechenden Windows 10 Lizenz ausgestattet werden. Für Desktop-Arbeitsplätze ist eine Windows 10 Pro Lizenz zu verwenden. Darüber hinaus kann für Notebook-Arbeitsplätze in Abhängigkeit der Netzanbindung eine Windows 10 Enterprise-Lizenz notwendig werden.

5.3.2 Microsoft Office

Dienstliche Geräte innerhalb der verfassten Kirche sollen nach Entscheidung des Anstellungsträgers mit einer entsprechenden Microsoft Office365 Lizenz aus dem mit Microsoft geschlossenen landeskirchlichen Rahmenvertrag ausgestattet werden. Ebenfalls steht den Nutzern im zentralen Nutzerportal der Landeskirche das Office365 zur Verfügung. Dieses Lizenzmodell ist ein Mietmodell und berechtigt immer zur Nutzung der aktuellen Software-Version.

Nutzungsberechtigt sind alle hauptamtlichen und ehrenamtlichen Mitarbeitenden der verfassten Kirche. Die Entscheidung über den Einsatz dieser Lizenz und die Finanzierung trifft der Anstellungsträger. Die Bereitstellung der Lizenzen erfolgt zentral durch die Landeskirche. Das Rollout und die Aktualisierung der Software erfolgt über unseren Infrastruktur-dienstleister. **Eine zentrale Finanzierung, bzw. Finanzierung über die jeweiligen Anstellungsträger ist zu prüfen und zu budgetieren.**

Die Lizenz ist an den Nutzenden gebunden und setzt voraus, dass der Anwender ein Konto im zentralen Nutzerverzeichnis der Landeskirche hat. Die Lizenzregistrierung erfolgt dann automatisch online über eine Verzeichnis-Kopplung zu den Microsoft-Servern. Auf dem gleichen Wege kann eine Lizenz nach Wegfall der Nutzungsberechtigung auch wieder wirksam deaktiviert werden, so dass eine unberechtigte Nutzung unterbunden wird.

5.3.3 Desktop Antivirus

Als Desktop Virenscanner wird im Bereich der Evangelisch-lutherischen Landeskirche Hannovers standardmäßig die aktuelle Kaspersky Security Suite eingesetzt. Die Lizenz ist

einsetzbar für die aktuellen Windows Desktop-Systeme sowie Windows Server. Der Einsatz des Virenscanners ist im zentralen Informationsverbund verpflichtend.

Die Lizenz wird zentral von der Landeskirche bereitgestellt. Das Rollout, Update, Management und Support der Lösung wird zentral durch unseren Infrastruktur-Dienstleister durchgeführt. Die Software sowie eine Installationsanleitung können von dem IT-Service Portal der COMRAMO AG heruntergeladen werden.

5.3.4 Fernwartung

Für eine Fernbetreuung der Arbeitsplätze ist eine Remote Desktop Software des Herstellers ISL Online vorgesehen. Diese Lösung arbeitet mit einer kleinen Software-Komponente auf dem PC-Arbeitsplatz, die dort abgelegt werden muss, und einem eigenen Gateway Server im Rechenzentrum unseres Infrastruktur-Dienstleisters. Die Software wird immer aktuell gehalten, ohne dass auf den Clients etwas nachinstallieren muss. Der Zugriff erfolgt verschlüsselt über das geschützte Kirchennetz oder über das Internet. Das Tool ist für alle gängigen Betriebssysteme konzipiert: Windows, Mac oder Linux Rechner. Auch mobile Geräte wie Android, IOS und Windows Phone werden in der aktuellsten Version unterstützt. Die Fernwartung wird nach Austausch eines Sitzungsschlüssels aufgebaut und ermöglicht einen Fernwartungs- und Fernzugriff mit Dateitransfer und Live Chat.

Diese Fernwartungslösung wird zentral durch die Landeskirche bereitgestellt. Die COMRAMO ist mit Aufbau und Hosting beauftragt. Ein Betrieb der Lösung ist ab 2018 geplant.

5.4 Arbeitsplatzverwaltung

Im Zuge der Stichproben und der Gespräche in den Kirchenämtern hat sich ein ganz unterschiedlicher Ausstattungsgrad offenbart. In vielen Dienststellen haben bereits Geräteerneuerungen stattgefunden, so dass eine generelle Neuausstattung nicht notwendig ist. Diese in Eigenregie angeschafften Geräte müssen in einem Nutzungskonzept separat betrachtet werden, so dass sich in Zukunft zwei unterschiedliche Verwaltungsszenarien für Arbeitsplatzgeräte ergeben.

Zusätzlich muss unabhängig von den beiden Nutzungsszenarien eine gemeinsame sichere Umgebung für die Arbeit mit dienstlichen Anwendungen und Daten in Form von virtuellen Arbeitsplätzen geschaffen werden.

5.4.1 Gemanagte Arbeitsplatzgeräte

Bei diesen Arbeitsplatzgeräten handelt es sich um rein dienstliche Geräte. Sie sollen unter Einhaltung landeskirchlicher Standardvorgaben aus dem definierten Warenkorb beschafft und ausgerollt werden. Die Rechner werden vor der Auslieferung mit der Standard-Software bespielt und vorkonfiguriert. Sie sind mit einem einheitlich konfigurierten Betriebssystem ausgestattet. Als Desktop-Betriebssystem kommt Windows 10 zum Einsatz.

Um einen stabilen Betrieb sicherzustellen, sind diese Arbeitsplätze komplett in das sichere Kirchennetz integriert. Sie sind im zentralen Nutzerverzeichnis registriert und die Anwender melden sich am zentralen Nutzerverzeichnis der Landeskirche an. Dabei soll eine Steuerung der Arbeitsplätze über Gruppenrichtlinien möglich sein, ebenso sind ein Rollout und eine Aktualisierung von Standard-Software über zentrale Update-Verfahren vorgesehen.

Für diese Standard-Software ist von der Landeskirche ein Verzeichnis zu definieren. Ein entsprechendes Updatesystem ist von unserem Infrastrukturdienstleister aufzubauen und laufend mit aktuellen Paketen zu versorgen.

Der Standard-Benutzer hat keine Administrationsrechte. Der Arbeitsplatz wird durch einen Systemadministrator oder einen beauftragten Vor-Ort-Dienstleister betreut. Der zuständige Vorort-Betreuer bekommt auf Anfrage ein lokales Admin-Passwort ausgehändigt, um ggf. lokal genutzte Software oder Treiber auf Fehler zu analysieren oder zu installieren. Bei Problemen mit der Netzanbindung, Authentifizierung oder zentral bereitgestellten Applikationen, die er nicht selbst lösen kann, wendet er sich an den Support des Infrastrukturdienstleisters. Bei Hardware-Problemen macht er im Rahmen seiner Wartungsverträge direkt eine Störungsmeldung beim Lieferanten auf.

Die Kommunikation in der gemanagten Umgebung findet stets über das gesicherte Kirchennetz statt. Zu diesem Zwecke wird der Arbeitsplatz über geeignete standardisierte VPN-Hardware- oder Software-Lösungen angebunden. Eine Verbindung in das Kirchennetz wird automatisch hergestellt, sobald der Anwender online und an seinem Arbeitsplatz angemeldet ist.

In diesem Rahmen ist online eine Anmeldung am zentralen Nutzerportal möglich, um auf dem bereitgestellten virtuellen Arbeitsplatz zentrale Standardapplikationen und Fachanwendungen zu nutzen. Bei Abmeldung von dem Nutzerportal wird nicht mehr in der zentralen Kirchennetz-Umgebung gearbeitet, sondern lokal. Hier kann sich der Nutzer von seinem Vorort-Dienstleister oder über ein zentral konfiguriertes Software-Verteilungssystem zusätzliche dienstliche Software individuell installieren lassen. Das schließt die Nutzung eines lokal installierten Office 365 mit ein. Sein dienstliches Home-Laufwerk sowie weitere Netzlaufwerke werden ihm im Explorer automatisch bei der Netzanmeldung eingebunden. Der Anwender arbeitet lokal in seiner dienstlichen Umgebung und nutzt primär die in seiner Dienststelle bereitgestellten Applikationen. Er greift auch mit seinem lokal installieren Outlook auf sein zentral betriebenes Exchange-Postfach zu.

Das Konzept setzt voraus, dass die zuständige Dienststelle ihren Anwendern einen Internet-Anschluss ihrer Wahl zur Verfügung stellt. Für den Anschluss ist die Dienststelle verantwortlich.

Der Internet-Zugriff kann direkt am Anschluss ausgekoppelt werden. Zur Absicherung dieses Zugriffs müssen Sicherheitsmechanismen greifen, die zentral durch den Infrastrukturdienstleister konfiguriert werden.

5.4.2 Ungemanagte Arbeitsplatzgeräte

Wenn eine Dienststelle keine zentral ausgerollten, vorkonfigurierten und administrierten Arbeitsplatzgeräte haben möchte, weil sie ihre Systeme bereits aktualisiert hat, keine zentralisierte Administration wünscht oder mit individuell beschaffter Software arbeiten möchte, so wird ihr die Möglichkeit zugestanden, mit ihrer eigenen Hardware zu arbeiten. Allerdings ergeben sich daraus deutliche Unterschiede in der Handhabung und das Gerät ist nicht Bestandteil des zentralen landeskirchlichen Informationsverbundes.

Ebenfalls muss in Betracht gezogen werden, dass im Rahmen der Gemeindearbeit viel Kommunikation mit Gemeindegliedern stattfindet und hier die gängigen Sozialen Netze und aktuelle Applikationen genutzt werden, um Informationen auszutauschen oder sich zu organisieren. Da viele dieser Produkte u.a. aus Datenschutzgründen nicht für den dienstlichen Einsatz geeignet sind, ist eine strikte und saubere Trennung zwischen den Daten aus sozialen Netzen und dienstlichen Daten unerlässlich. Die Trennung wird in diesem Szenario umgesetzt.

Die Arbeitsplätze werden außerhalb des sicheren Kirchennetzes betrieben und behandelt wie unbekannte Rechner. Hier findet keine Registrierung des Gerätes an der zentralen Domain statt. Eine Steuerung oder zentrale Betankung mit Software erfolgt nicht. Der Anwender ist für die Administration und auch die Sicherheit seines Gerätes komplett selbst verantwortlich.

Der Anwender kann ein Betriebssystem seiner Wahl auf dem Arbeitsplatz betreiben. Es muss nur dem aktuellen Stand der Technik entsprechen und kompatibel sein zu den Anwendungen, die für den Kirchennetz-Zugriff installiert werden. Das sind eine Zugangssoftware zum virtuellen Arbeitsplatz im Nutzerportal, die Fernwartungssoftware sowie eine Software zur sicheren Netzanbindung.

Das Konzept setzt voraus, dass die zuständige Dienststelle ihren Anwendern einen Internet-Anschluss ihrer Wahl zur Verfügung stellt. Der Internet-Zugriff erfolgt direkt am Anschluss der Dienststelle. Für den Anschluss sowie die Sicherheit des lokalen Systems ist die Dienststelle selbst verantwortlich.

Der Anwender arbeitet lokal auf seinem Arbeitsplatz in seiner individuellen Umgebung und mit seinen individuellen Programmen. Für den korrekten Betrieb seines Arbeitsplatzes ist der Anwender selbst verantwortlich.

Wenn der Anwender zentral bereitgestellte dienstliche Standardapplikationen nutzen möchte, dann stellt er über die installierte Zugangssoftware eine sichere Verbindung zum Rechenzentrum her und meldet sich über das Nutzerportal an seinem virtuellen Arbeitsplatz an. Dort hat er neben seinen Officeprogrammen auch Zugriff auf sein Exchange-Postfach über Outlook sowie auf alle zentralen Fachapplikationen, die für ihn eingerichtet sind. Die Nutzung von dienstlichen Daten und Applikationen innerhalb des Kirchennetzes ist für ungemanagte Arbeitsplatzrechner nur über dieses Portal möglich.

Um eine Trennung zwischen dienstlichen und individuellen Daten zu erreichen, müssen – sofern erforderlich - lokal gespeicherte dienstliche Dokumente in einer Containerlösung abgelegt oder anderweitig verschlüsselt werden.

Zum datenschutzkonformen Umgang mit dienstlichen Daten muss mit dem Anwender eine Nutzervereinbarung geschlossen werden. Ein derartiges Dokument muss zeitnah entwickelt werden.

6. Anbindung an das Kirchennetz

Das vorhandene Konzept des Kirchennetzes wird grundlegend erweitert. Bisher gab es nur den Ansatz der voll gemanagten Arbeitsplatzgeräte, die sich in einer rein dienstlich verwalteten Umgebung bewegt haben. Dieses Konzept wird erweitert durch das Szenario der ungemanagten Arbeitsplatzgeräte.

Die Netzanbindungsszenarien müssen für Standorte mit mehreren Arbeitsplätzen und für Einzelarbeitsplätze betrachtet werden. Soll ein Mischbetrieb von gemanagten und ungemanagten Arbeitsplatzgeräten innerhalb eines Standortes stattfinden, so müssen geeignete Maßnahmen ergriffen werden, die einen sicherheitstechnisch unzulässigen Datenzugriff zwischen diesen beiden Formen reglementieren, z.B. durch den Betrieb in voneinander getrennten Teilnetzen.

6.1 Anbindung von Standorten an das Kirchennetz

Ziel

Ziel ist es, allen gemanagten Arbeitsplätzen in einem dienstlichen Verwaltungsnetz mit Hilfe einer Hardware-Lösung einen sicheren und transparenten Zugriff auf alle Ressourcen und Applikationen zu ermöglichen, auf die sie im Rahmen ihrer Befugnisse zugreifen dürfen. Das können sowohl zentral gehostete Ressourcen im Rechenzentrum sein als auch Applikationen im zuständigen Kirchenamt. Außerdem müssen auch Applikationen und Ressourcen von Arbeitsplätzen aus dem Kirchennetz erreichbar sein, die in der Dienststelle betrieben werden. Auf eine ausreichende Bandbreite und eine Ausfallsicherheit ist besonders Wert zu legen.

Nutzen

Notwendig ist ein standardisierter Zugriff, der mit Hilfe einer Hardware-Lösung unabhängig von der eingesetzten Festnetz-Leitungstechnik (Festanbindung, EtherConnect, aDSL, aDSL-Bündelung, VDSL) flexibel mit Anschlüssen beliebiger Internetanbieter betrieben werden soll. Die Lösung ermöglicht einen stabilen, ausfallsicheren und performanten Zugriff, ohne dass Software auf den Arbeitsplätzen installiert werden muss. Derart angebundenen Dienststellen sind in der Lage, lokale Serverstrukturen zu betreiben und diese über einen permanenten bidirektionalen VPN-Tunnel auch Arbeitsplätzen außerhalb Ihres LANs über das Kirchennetz zur Verfügung zu stellen. In Verbindung mit der aktuellen Hardware und der einheitlichen Betriebssystemumgebung ist eine effektive Verwaltung dieser Systeme gegeben.

Umsetzung

Das IT-Referat des Landeskirchenamtes berät bei der Auswahl der geeigneten Bandbreite und der Leitungsanbindung. Die Internet-Leitung wird von der Dienststelle eigenverantwortlich beschafft und betrieben. Die Anbindung an das Kirchennetz wird von unserem Infrastrukturdienstleister mit Hilfe von standardisierter Router-Hardware realisiert. Die Hardware wird passend zur Bandbreite des vor Ort zur Verfügung stehenden Internet-Anschlusses dimensioniert und den Dienststellen angeboten. Die Bereitstellung erfolgt vorkonfiguriert. Die Inbetriebnahme wird von der zuständigen Systembetreuung vor Ort oder von einem beauftragten Dienstleister vorgenommen. Der Router bleibt nach Inbetriebnahme in der Verwaltungshoheit des Infrastrukturdienstleisters. Eine laufende Betreuung sowie ein entsprechender Austauschservice innerhalb eines Werktages müssen möglich sein.

Diese Lösung ist bereits im Einsatz. Eine Überarbeitung der Produktpalette wird zurzeit von der COMRAMO vorgenommen. Mit einem Abschluss ist im ersten Halbjahr 2018 zu rechnen. Parallel finanziert die Landeskirche seit mehreren Jahren zentral eine jeweils zweite Leitung (MPLS) der Kirchenämter zur Comramo, um eine ausfallsicheres Arbeiten an zentralen Applikationen zu gewährleisten.

6.2 Anbindung von gemanagten Einzelplätzen an das Kirchennetz

Ziel

Ziel ist es, gemanagten Einzelarbeitsplätzen mit Hilfe einer Software-Lösung innerhalb einer rein dienstlichen Umgebung automatisch einen sicheren und transparenten Zugriff auf alle Ressourcen und Applikationen zu ermöglichen, auf die sie im Rahmen ihrer Befugnisse zugreifen dürfen. Das können sowohl zentral gehostete Ressourcen im Rechenzentrum sein als auch Applikationen im zuständigen Kirchenkreisamt. Die Lösung soll in Verbindung mit der lokalen Internet-Auskopplung und der Zwei-Faktor Authentisierung flexibel einsetzbar sein, trotzdem einen definiert hohen Sicherheitsstandard bieten.

Nutzen

Der Zugriff soll über eine unabhängig von der eingesetzten Anschlusstechnik (LAN, Modemeinwahl, UMTS/LTE, WLAN oder öffentlicher Hotspot) flexibel möglich sein. In Verbindung mit der aktuellen Hardware und der einheitlichen Betriebssystemumgebung muss eine effektive Verwaltung dieser Systeme inklusive Software Aktualisierungen möglich sein. Der Anwender meldet sich in der Domäne an und bekommt automatisch einen Zugriff auf das Kirchennetz und alle Ressourcen, sobald er online ist. Ein Zugriff auf die Citrix-Farm ist ebenfalls möglich.

Umsetzung

Ein geeignetes System muss aufgebaut werden, das es dem Nutzer unabhängig vom Standort ermöglicht, bei der Anmeldung an seinem Arbeitsplatz automatisch und ohne zusätzliche Aktionen eine Domain-Anmeldung vorzunehmen und eine sichere Verbindung zum Kirchennetz herzustellen. Außerdem muss geprüft werden, wie ein Verfahren zur Administration, Bestellung, Rollout und laufender Pflege von gemanagten Arbeitsplätzen implementiert werden kann.

Entsprechende technische Lösungen werden vom IT-Referat des Landeskirchenamtes in Zusammenarbeit mit der COMRAMO evaluiert. Der Aufbau und die Bereitstellung dieser Infrastruktur wird für Ende 2018 angestrebt.

6.3 Direkte Internet-Auskopplung am lokalen Internetanschluss

Ziel

Um die vorhandene Anschlussbandbreite voll nutzen zu können und auch um den VPN-Verkehr zu minimieren, soll der Internet-Verkehr nicht mehr über den zentralen Breakout beim zentralen Infrastrukturdienstleister geroutet werden, sondern vor Ort ausgekoppelt werden. (Split-Tunneling). Ziel ist es, den für das Internet bestimmten HTTP- und HTTPS-Datenverkehr ohne Sicherheitseinbußen direkt am Anschluss des Anwenders auszukoppeln und direkt ins Internet zu ausleiten. Alle Aspekte des Datenschutzes und der IT-Sicherheit müssen gewahrt bleiben.

Nutzen

Neben der höheren Zugriffsgeschwindigkeit soll eine deutliche Flexibilisierung der Internet-Nutzung und damit eine deutlich höhere Nutzerzufriedenheit erreicht werden. Auf notwendig werdende kostspielige Erweiterungen der Hardware und zentraler Datenleitungen kann verzichtet werden, da durch diese Lösung eine Lastreduzierung auf den VPN-Verbindungen erzielt werden kann. Zentrale Systeme werden nicht mehr so stark belastet und können ggf. mit deutlich weniger komplexen Konfigurationen ausgestattet werden.

Umsetzung

Durch die lokale Auskopplung des Internet-Verkehrs werden einige Sicherheitsfunktionen des zentralen Internet-Zugangs nicht mehr genutzt. Dafür muss eine lokale Lösung eingesetzt werden. Diese kann für LAN-Anbindungen als Hardware implementiert werden und für Einzelplatz-Anbindungen als Software. Die Lösung muss eine Firewall implementieren, mit der eine zentral administrierbare Steuerung der Zugriffsberechtigungen realisiert werden kann Ein URL-Filter muss konfigurierbar sein, um beim Internet-Zugriff den Jugendschutz-Vorschriften zu genügen. Ebenso muss der Zugriff auf Bot-Netze erkannt und unterbunden werde. Ein Schutz vor Zero-Day Exploits muss implementiert sein.

Eine geeignete Hardware-Lösung wird momentan getestet und die Nutzung der vorhandenen Virenscanner-Lösung für den Einsatz in diesem Szenario geprüft. Eine Beendigung des Tests wird bis Mitte 2018 angestrebt. Danach folgt eine Entscheidung über die Einführung.

6.4 Anbindung von ungemanagten Einzelplätzen

Ziel

Ziel ist es, von nichtverwalteten Individual- bzw. Fremdsystemen den Zugriff auf das zentrale landeskirchliche Nutzerportal zu ermöglichen, ohne die IT-Informationssicherheit in der Kirchennetz-Infrastruktur zu gefährden. Dieses Vorgehen ermöglicht es auch, zentral gehaltene dienstliche Daten und Applikationen streng von den nichtdienstlichen lokalen Daten zu trennen.

Nutzen

Dieses Vorgehen erlaubt es den Nutzenden, ihre bereits vorhandene/eigene Hardware an die LAN-Infrastruktur anzubinden. Es muss nicht von zentraler Stelle ein neues Gerät beschafft werden. Außerdem können die Nutzenden ihre eigene individuelle Software auf dem Arbeitsplatz betrieben, ohne dass es zu sicherheitsrelevanten Problem führt. Ein solcher Arbeitsplatz kann als Einzelplatzlösung angebunden sein (z.B. mobil, WLAN, Hotspot) oder in einem Fremdnetzwerk stehen. Diese Möglichkeit dürfte der Interessenlage unserer Pastorenschaft entsprechen, die mit selbst erworbenen (u.U. durch die Landeskirche finanziell unterstützten) Arbeitsplatzgeräten dienstlich arbeiten möchten.

Umsetzung

Ein geeignetes System muss aufgebaut werden, um bei Bedarf eine verschlüsselte Datenverbindung zum zentralen Nutzerportal der Landeskirche aufzubauen. Ein anderer Zugriff in das Kirchennetz außer auf das zentrale Nutzerportal soll nicht möglich sein. Die annehmenden Gateways müssen hochverfügbar betrieben werden.

Der Anwender meldet sich mit seinen im zentralen Nutzerverzeichnis hinterlegten Zugangsdaten am System an. Zum Schutz der zentralen Infrastruktur soll ein Compliance-Check durchgeführt werden. So könnte das Vorhandensein einer lokalen Firewall und eines Virenscanners erfolgreich geprüft werden, bevor der Zugriff auf das Portal gewährt wird.

Die notwendige Client-Lösung muss als (vorkonfiguriertes) Paket für die Betriebssysteme Windows, Apple iOS und Android zum Download zur Verfügung gestellt werden. Ebenfalls muss eine Installationshilfe bereitgestellt werden. Nur für die zentral zur Verfügung gestellt Software ist ein Anwendersupport zu leisten. Sonstige lokal installierte Software ist vom Anwender in Eigenregie zu betreiben.

Entsprechende technische Lösungen müssen noch durch das IT-Referat des Landeskirchenamtes evaluiert werden. Der Aufbau und die Bereitstellung dieser Lösung durch den Infrastrukturdienstleister COMRAMO werden für Ende 2018 angestrebt.

6.5 Kirchennetzzugriff über Mobilanbindung

Ziel

Ziel ist es, den Nutzerinnen und Nutzern einen mobilen Zugriff auf dienstliche Informationen innerhalb eines verbindlich definierten Rahmens zu ermöglichen.

Nutzen

Zusätzlich zum PC-Arbeitsplatz haben viele Nutzerinnen und Nutzer häufig noch ein mobiles Endgerät zur Verfügung. Das kann ein entweder dienstliches oder privates Smartphone oder ein Tablet sein, mit dem von unterwegs gearbeitet wird.

Damit muss von Unterwegs ein Zugriff auf das Mailpostfach möglich sein, um Emails, Termine, Kontakte und Aufgaben abrufen zu können. Per Email empfangene Office- und Acrobat-Anlagen müssen geöffnet und bearbeitet werden können. Zusätzlich muss der Zugriff auf das Internet und der Datenaustausch mit einem persönlichen dienstlichen Cloud-Laufwerk möglich sein. Weitere kirchliche Applikationen müssen sich installieren lassen.

Umsetzung

Um eine Verwaltung der dienstlichen Arbeitsumgebung zu ermöglichen, muss das mobile Endgerät an ein zentrales Verwaltungssystem angebunden werden. Diese Verwaltungsumgebung muss sowohl über das Internet als auch über das Kirchennetz erreichbar sein. Über dieses zentrale Verwaltungssystem müssen die grundlegenden Sicherheitsfunktionen administrierbar sein. Wenn dienstliche Daten auf dem Endgerät gespeichert werden, dann müssen sie verschlüsselt abgelegt werden, um eine Vertraulichkeit auch im Falle eines Verlustes zu gewährleisten. Jedes Endgerät mit dienstlichem Einsatzzweck muss durch einen Zugangscode vor Fremdzugriff gesichert werden („Sperrfunktion"). Nach Beendigung des Dienstverhältnisses oder bei Verlust des Endgerätes muss es die Möglichkeit geben, die dienstlichen Daten auf dem Gerät zu löschen bzw. unbrauchbar zu machen. Dienstliche Daten müssen derart abgesichert werden, dass sie nicht von nichtdienstlichen Applikationen ausgelesen werden können.

Für rein dienstliche Geräte gibt es bereits Zugangsmöglichkeiten über spezielle Providerverträge. Die Mobilzugänge werden vom zentralen Infrastrukturdienstleister verwaltet. Die Einwahl erfolgt direkt über einen zugeordneten Einwahlpunkt (APN) in das sichere Kirchennetz. Auf diesen Geräten darf es nur dienstlich bereitgestellte Applikationen und Daten geben, eine private Nutzung ist ausgeschlossen.

Ungemanagte dienstlich zur Verfügung gestellte Geräte oder eigenbeschaffte Endgeräte erhalten über einen beliebigen Mobilfunkvertrag, den der Nutzer individuell abgeschlossen hat, Zugriff auf das Internet.

Da auf diesen Geräten die Nutzung zusätzlicher individueller Software möglich ist, muss eine Trennung der dienstlich bereitgestellten von den individuellen Informationen stattfinden. Zusätzlich ist mit den Nutzern eine entsprechende Nutzungsvereinbarung zu treffen, die Fragen der Haftung, der Fernverwaltung und des datenschutzkonformen Umgangs mit dienstlichen Daten regelt. Ein solches Vertragsmuster ist zu entwickeln.

Die zentrale Bereitstellung einer bei der COMRAMO gehosteten Geräteverwaltung sowie einer Nutzungsvereinbarung wird bis Ende 2018 angestrebt.

6.6 Kommunikation mit Ehrenamtlichen

Ziel

Ziel ist eine Optimierung der Zusammenarbeit der Kirchengemeinden mit ehrenamtlichen Gremienmitgliedern und eine Aufwertung der ehrenamtlichen Arbeit.

Nutzen

Durch die Schaffung von standardisierten Plattformen für den Informationsaustausch wird die Kommunikation in der Gemeindearbeit deutlich verbessert. Daten können im Rahmen von definierten Arbeitsgruppen mit gemeinsamem Zugriff in einer definierten, strukturierten kirchlichen Umgebung an zentraler Stelle abgelegt werden.

Eine Bereitstellung von IT für Ehrenamtliche trägt dem Stellenwert der ehrenamtlichen Gremienmitglieder Rechnung. Durch eine auch hier vereinheitlichte Infrastruktur könnten die Arbeit mit Dateien und Dokumenten erleichtert werden, auch die zentrale Bereitstellung aktueller Adressdaten würde vereinfacht werden. Den Aspekten des Datenschutzes würde überdies Rechnung getragen, wenn dienstliche Daten innerhalb der kirchlichen Infrastruktur verbleiben würden.

Umsetzung

Mit dem Produkt intern-e ist eine Austausch und Kommunikationsplattform in der Landeskirche etabliert, in der sich Haupt- und Ehrenamtliche austauschen können. Dies wird auch in 2018 um Funktionalitäten erweitert. Auf dieser Plattform werden geschlossene Arbeitsgruppenbereiche mit allen Haupt- und Ehrenamtlichen für die Gemeinden definiert. Innerhalb dieser Arbeitsgruppenbereiche können die Teilnehmenden zentral Informationsseiten schalten, Dokumente ablegen, Terminkalender pflegen oder miteinander Chatten. **Dieses System existiert bereits. Die technische Betreuung erfolgt durch die Kommunikationsabteilung.**

Parallel zum Angebot von intern-e wird überlegt, im Rahmen der Kirchenvorstandswahl ehrenamtlichen Gremienvertretern auch ein dienstliches Email-Postfach zu geben. Hierfür müssen die Gremienmitglieder der Gemeinden erfasst und in das zentrale Nutzerverzeichnis eingepflegt werden. Über eine webbasierte Bereitstellung ist nicht nur das Empfangen und Senden von Emails möglich, sondern auch das Online-Bearbeiten von Dokumenten.

Eine Bereitstellung dieser Office-Online Plattform durch die Landeskirche kann in 2018 erfolgen.

7. Arbeitsplatzbetreuung / Support

Ziel

Optimale Unterstützung der hauptamtlichen Mitarbeiter in der Landeskirche bei der Bewältigung auftretender IT-Probleme innerhalb des zentralen Informationsverbundes. Dies beinhaltet die gemanagten Geräte sowie die Anbindung von nicht gemanagten Geräten, nicht aber die ungemanagten Geräte selbst.

Nutzen

Die Anwender haben in der Regel weder die Qualifikation noch die Zeit, um sich mit IT-Problemen auseinanderzusetzen. Es werden feste Ansprechpartner benötigt, die im Fehlerfall kontaktiert werden können und die zeitnah bei Problemen helfen und eine Lösung herbeiführen können. Die Dienstleister müssen die aufgetragenen Arbeiten konform zu den geltenden Regelungen und den Konzepten der Landeskirche durchführen. Im Zweifelsfall ist eine Klärung mit der zentralen IT der Landeskirche bzw. dem Infrastrukturdienstleister notwendig.

Umsetzung

Nach einer technischen und organisatorischen Abgrenzung des Informationsverbundes sind Regelungen zu den Zuständigkeiten der jeweiligen Administratoren und der ggf. eingeschalteten Dienstleister zu treffen. Um einen angemessenen Support leisten zu können, muss es regelmäßige Informationen und Schulungen für alle Teilnehmer geben, in denen Standards und Konzept der Landeskirche vermittelt werden.

Die Landeskirche bietet in Zusammenarbeit mit dem zentralen Infrastrukturdienstleister ein Partnernetzwerk an. Ziel ist es, eine Verbesserung der Zusammenarbeit und der Betreuungsleistung mit externen Dienstleistern zu erreichen, die die Körperschaften und Einrichtungen unterstützen. In diesem Rahmen ist beabsichtigt, regelmäßige Informationen, Veranstaltungen und Workshops angeboten. Um daran partizipieren zu können, muss sich ein Dienstleister im Partnernetzwerk registrieren und die Informationsangebote wahrnehmen. **Erste Workshops hierzu haben bereits stattgefunden. Für die erste Jahreshälfte 2018 sind Schulungen zum Umgang mit dem Fernwartungsprogramm geplant.**

7.1 Zentrale Hotline durch den Infrastruktur-Dienstleister

Für alle Netz- und Hosting- Dienstleistungen für gemanagte Arbeitsplätze im sicheren Kirchennetz gibt es einen zentralen, für alle Nutzenden zugänglichen einheitlichen Support des zentralen Infrastrukturdienstleisters. In diesem Rahmen wird allen Anwendern der Landeskirche eine zentrale Hotline (User Helpdesk) unter einer Service-Rufnummer zur Verfügung gestellt. Eine Call-Annahme erfolgt rund um die Uhr an 365 Tagen im Jahr. Darüber hinaus sind Servicezeiten und Reaktions- und Lösungszeiten definiert, in denen eine Entstörung durchgeführt wird.

7.2 Lokaler Support durch Systemverwalter

Jedes Kirchenamt hat einen oder mehrere IT-Zuständige, genannt Systemverwalter, die in der Einrichtung entweder mit einer ganzen Stelle oder nur mit einer Teilstelle die IT-relevanten Betreuungsaufgaben vor Ort wahrnehmen. Betreuungsumfang und Intensität ist in jedem Kirchenamt individuell geregelt.

In der Regel stellen die Systemverwalter den ersten Ansprechpartner dar, um individuell ein Problem zu lösen oder vorzuklären und wenn nötig eine qualifizierte Problemmeldung an Dritte wie Leitungsanbieter und Hardware-Lieferanten abzugeben.

Die Systemverwalter bilden auch die Schnittstelle zum Infrastruktur-Dienstleister bei zentralen Problemen und Fragestellungen. Hierbei haben sie die Aufgabe der Vorklärung des Problems sowie der Unterstützung bei der lokalen Entstörung.

Das Aufgabenverzeichnis der Kirchenämter wird momentan überarbeitet. **Eine Betreuung der Kirchengemeinden durch die Systemverwalter und die Wahrnehmung der Verantwortung der IT im Bereich der Verwaltungsbezirke durch die jeweiligen Verwaltungsämter ist zwingender Bestandteil des IT-Konzeptes.**

7.3 Betreuung durch externe Servicepartner vor Ort

In Abstimmung mit der jeweiligen Kirchenverwaltung können kirchliche Stellen bestimmte IT-relevante Betreuungsaufgaben, die vor Ort anfallen, ganz oder auch nur teilweise an externe Servicepartner outsourcen. Das können Einzelaufträge sein oder auch längerfristige Supportverträge. In der Regel bilden auch hier die Systemverwalter in den Kirchenämtern die steuernde Schnittstelle zum jeweiligen Servicepartner.

Voraussetzung für ein Auftragsverhältnis muss eine schriftliche Vereinbarung über die Verarbeitung personenbezogener Daten (ADV) und der Abschluss einer IT-Dienstleistungsvereinbarung sein. Diese IT-Dienstleistungsvereinbarung beinhaltet zusätzliche Regelungen zur Zusammenarbeit im Partnernetzwerk, der Informationssicherheit

und der Geheimhaltung und wird als ergänzende Regelung zur Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß § 11 Datenschutzgesetz-EKD (DSG-EKD) getroffen. **Die Entwicklung und Bereitstellung eines Mustervertrages wird bis Mitte 2018 angestrebt.**

8. Projekt- und Kostenplanung

Die Umsetzung des IT-Konzeptes 2020 lässt sich in mehrere Phasen gliedern, die aufeinander aufbauen.

8.1 Phase 1: Schaffung der rechtlichen Grundlagen

Die vorliegende Planung setzt voraus, dass zeitnah ein rechtlicher Rahmen geschaffen wird, der die Nutzung der IT in der Landeskirche verbindlich regelt und die Grundlage für alle weiteren Überlegungen darstellt. Ein entsprechendes Kirchengesetz sollte bis Frühjahr 2018 vorbereitet und dann von der Synode verabschiedet werden. Es sollte u.a. folgende Aspekte regeln:

- Regelung des Geltungs- und Anwendungsbereiches u.a. zur Feststellung des Umfangs der Maßnahmen.
- Vorgabe einer verbindlichen Teilnahme am landeskirchlichen IT-Verbund sowie Teilnahme am zentralen Nutzerverzeichnis und dem zentralen Mailsystem.
- Definition von Standards hinsichtlich der Infrastruktur und der zu verwendenden Softwareprodukte.
- Festlegung der Finanzierung. Zentrale Infrastrukturen und Standards sollten von der Landeskirche finanziert werden, dezentrale Dienste sowie nutzerabhängige Leistungen sollten dezentral durch die jeweiligen Anstellungsträger finanziert werden.
- Regelung der organisatorischen Zuständigkeiten im IT-Verbund, insbesondere hinsichtlich der Finanzierung und Betreuung von Kirchenämtern, Gemeinden und Ehrenamtlichen.
- Festlegung von Nutzungsrichtlinien, die eine sicherheits- und datenschutzkonforme Nutzung der IT sicherstellen.
- Definition einer Übergangsfrist für alle Regelungen, um einen definierten Zieltermin zu erhalten. Vorstellbar wäre hier Ende 2022.

Diese rechtlichen Grundlagen stellen die Voraussetzung für eine valide Zeit- und Kostenplanung dar, die im Anschluss erfolgen muss. Ohne Kenntnis des Umfanges und können keine verlässlichen Zahlen genannt werden.

8.2 Phase 2: Evaluierung und Aufbau der notwendigen Infrastruktur

Eine Detailplanung zur Umsetzung des Konzeptes muss noch erstellt werden. Die Umsetzung gliedert sich in mehrere Projekte, die sich derzeit in der Angebots- und Evaluierungsphase befinden. Nachfolgend wird für die wichtigsten Projekte eine grobe Zeitplanung und Kostenschätzung dargestellt.

Projekt	Abschluss bis	Projektkosten
A) Kirchennetz	Ende 2018	500.000
B) Aufbau zentrales Portal und	Ende 2018	250.000
B) Aufbau virtuelle Arbeitsplatzumgebung	Ende 2018	250.000
C) AD und Email	Ende 2022	1.250.000
D) Gremienanbindung neue KVs - erstes Jahr	Frühjahr 2018	200.000
E) Geräte - Aufbau einer Infrastruktur zur Bereitstellung (Shop, Bestellverfahren, …)	Ende 2018	200.000
		2.650.000

Dabei handelt es um grob geschätzte **einmalige Projektkosten**, die durch die Realisierung der Lösungen entstehen, und **nicht um laufende** Kosten. Die Beschaffung und der Rollout von arbeitsplatzbezogener Hardware, Software oder Lizenzen ist ebenfalls noch nicht berücksichtigt. Präzisere Aussagen können erst nach weiterem Planungsfortschritt getroffen werden.

A) Kirchennetz

Projektschritte	Projektzeitraum
Anbindung von Standorten - Überarbeitung der Produktpalette (COMRAMO) - Bereitstellung bei Neubeauftragungen und Produktwechsel (COMRAMO)	bis 12/2017
Bereitstellung einer standardisierten Fernwartungslösung - Definition der Umgebung und Funktionen (LKA+COMRAMO) - Beschaffung Lizenzen und Wartungsverträge (LKA) - Aufbau und Bereitstellung des Fernwartungsservers (COMRAMO)	Bis 01/2018
Rollout der Fernwartungslösung - Freischaltung Nutzung durch alle definierten Systemadministratoren und Dienstleister (COMRAMO) - Schulung der Administratoren (COMRAMO)	Ab 02/2018 02/2018 bis 06/2018
Anbindung gemanagter Einzelarbeitsplätze - Evaluierung von VPN-Anbindungslösungen (LKA+COMRAMO) - Entscheidung über Einsatz und Produktauswahl (LKA) - Feinkonzeption (LKA+COMRAMO) - Aufbau und Bereitstellung der VPN-Lösung	 Bis 03/2018 Bis 03/2018 Bis 09/2018 Bis 12/2018

Direkte Internet-Auskopplung - Evaluierung von Hard- und Software-Lösungen (LKA+COMRAMO)) - Entscheidung über Einsatz und Produktauswahl (LKA) - Feinkonzeption (LKA+COMRAMO) - Bereitstellung der Software-Sicherheitslösung - Bereitstellung der Hardware-Sicherheitslösung	 Bis 03/2018 Bis 03/2018 Bis 09/2018 Bis 12/2018 Bis 12/2018
Anbindung ungemanagter Endgeräte - Definition des Feinkonzeptes (LKA+COMRAMO) - Implementierung der Lösung (COMRAMO)	 Bis 06/2018 07/2018 bis 12/2018
Anbindung mobiler Endgeräte - Definition der Anforderungen (LKA) - Entscheidung über Zuständigkeiten bei der Verwaltung der Endgeräte (Synode) - Evaluierung einer MDM und MAM-Lösung - Entscheidung über Einsatz und Produktauswahl (LKA) - Feinkonzeption (LKA+COMRAMO) - Aufbau und Bereitstellung der mobilen-Lösung (COMRAMO)	 Bis 03/2018 Bis 05/2018 03/2018 bis 06/2018 Bis 06/2018 07/2018 bis 10/2018 Bis 12/2018

B) Aufbau zentrales Portal und virtuelle Arbeitsplatzumgebung

Projektschritte	Projektzeitraum
Konzeption des zentralen Netscaler Nutzerportals (LKA)	01/2018 bis 09/2018
Definition eines virtuellen Arbeitsplatzstandards - Festlegung der Standard-Software (LKA+IT-Ausschuss)	03/2018 bis 09/2018
Aufbau und Bereitstellung des zentralen Nutzerportals mit den virtuellen Arbeitsplätzen (COMRAMO)	10/2018 bis 12/2018

C) Nutzerverzeichnis und E-Mail

Projektschritte	Projektzeitraum
Aufbau einer einheitlichen webbasierten Nutzerverwaltung - Auswahl und Beschaffung Software (LKA) - Erstellung eines Feinkonzeptes+Angebot (n.n.) - Aufbau und Bereitstellung des Systems (n.n.+COMRAMO)	01/2018 bis 12/2018

D) Gremienanbindung der neuen Kirchenvorstände

Projektschritte	Projektzeitraum
Entscheidung über Finanzierung (Synode)	Bis 05/2018
Definition landeskirchliche Maildomain	06/2018 bis 09/2018
Bereitstellung Online-Struktur - Anbindung Nutzerverzeichnis (COMRAMO) - Einrichtung Email-Domain (COMRAMO) - Definition und Umsetzung eines Workflows für die Benutzerpflege in Kirchenkreisen (LKA+Kirchenämter)	07/2018 bis 12/2018

E) Geräteausstattung

Projektschritte	Projektzeitraum
Definition eines Gerätestandards für Arbeitsplatzhardware (LKA)	Bis 03/2018
Entscheidung über Finanzierung (Synode)	Bis 05/2018
Entscheidung für Hardware-Hersteller (LKA) - Schließen von Rahmenverträgen (LKA) - Festlegung eines Warenkorbes (LKA+Hersteller) - Aufbau eines Shopsystems und eines Bestellworkflows (LKA+Hersteller)	04/2018 bis 12/2018
Definition eines Arbeitsplatzstandards - Festlegung der Standard-Software (LKA+IT-Ausschuss) - Erarbeitung eines Standard-Images und eines Verfahrens für initiale Software-Betankung durch den Hersteller (LKA+Hersteller)	07/2018 bis 12/2018
Arbeitsplatzmanagement und Lifecycle (COMRAMO) - Konzeption einer Arbeitsplatzverwaltung (COMRAMO) - Implementierung eines Software-Betankungssystems (COMRAMO)	07/2018 bis 12/2018
Bereitstellung einer Bestellmöglichkeit und des Betriebes standardisierter und gemanagter Arbeitsplätze	Ab 01/2019

8.3 Phase 3: Migration der Nutzer

Aufwand, Umfang und Dauer sind direkt abhängig von den in Phase 1 getroffenen Entscheidungen und Regelungen. Weitere Planungen können daher erst im Anschluss stattfinden.

8.4 Phase 4: Weitere Ausbaustufen

Die bisher beschriebenen Teilprojekte stellen die Grundlage für die Bereitstellung und den Betrieb des neuen landeskirchlichen Informationsverbundes dar. Noch nicht betrachtet sind weitere Ausbaustufen, die für sich gesehen wichtige Folgeprojekte darstellen. Dazu gehören unter anderem:

- Email-Verschlüsselung
- Email-Archivierung
- Email-Signaturlösung
- 2-Faktor-Authentifizierung
- Dienstliches Cloud-Laufwerk

8.5 Betriebsphase: Laufende Kosten

Die laufenden Betriebskosten sind direkt abhängig von den in Phase 1 getroffenen Entscheidungen und Regelungen. Weitere Planungen können daher erst im Anschluss stattfinden.