Auszug

aus dem Protokoll der 17. Sitzung des Kirchenkreisrates Lübeck-Lauenburg
vom 21. Oktober 2019

Zu der heutigen Sitzung ist vom vorsitzenden Mitglied rechtzeitig unter Angabe der Tagesordnung schriftlich eingeladen worden.

Es sind 9 Mitglieder erschienen.

Anwesende:

Vorsitzende:	Eiben
die Damen:	Weiß
die Herren:	Bretzke, Feddersen, von Kiedrowski, Römer, Schröder, Schuback, Dr. von Wedel

Der Kirchenkreisrat besteht aus 10 Mitgliedern. Die Versammlung ist demnach beschlussfähig.
Die Sitzung wird vor Eintritt in die Tagesordnung mit Gottes Wort und Gebet eröffnet.

Beginn der Sitzung 16.30 Uhr

2.2	**IT-Sicherheitskonzept**
	Beschluss (einstimmig) Der Kirchenkreisrat beschließt das vorgelegte Sicherheitskonzept für den Ev.-Luth. Kirchenkreis Lübeck-Lauenburg und bittet die Verwaltungsleitung, die Verfahrensverzeichnisse für die Fachverfahren erstellen zu lassen.

V. g. u.

gez: Kai Schröder
(stellvertr. Vorsitzender)

gez. Sandra Jäkel
(Protokollantin)

Die Richtigkeit des Auszugs wird beglaubigt:

L.S.

Kai Schröder
(stellvertr. Vorsitzender)

Lübeck, 29. Oktober 2019

Verfügung/en:
1. V Bu-Rei zK + zwV
2. neue Akte 9.8.5 IT-Sicherheitskonzept zdA

IT-Sicherheitskonzept

für den Evangelisch-Lutherischen Kirchenkreis Lübeck-Lauenburg

Inhalt

1 IT-Sicherheitskonzept

1.1 An wen wendet sich dieses Konzept?

Das IT-Sicherheitskonzept (Sicherheitskonzept) wendet sich an alle Mitarbeitenden sowie Angehörige des Evangelisch-Lutherischen Kirchenkreises Lübeck-Lauenburg.

1.2 Allgemeines

1.2.1 Anwenderqualifizierung

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Verantwortliche

Die Mitarbeitenden sind aufgabenspezifisch zu schulen und dürfen erst dann mit IT-Verfahren arbeiten. Anweisungen und Anleitungen durch Key-User, Handbücher und Dienstanweisungen sind zu beachten. Dabei sind Mitarbeitende insbesondere auch mit den für sie geltenden Sicherheitsmaßnahmen und den Erfordernissen des Datenschutzes vertraut zu machen.

Die Schulung hat prinzipiell auch das allgemeine Sicherheitsbewusstsein und die Einsicht in die Notwendigkeit von IT-Sicherheitsmaßnahmen zu entwickeln. Die Schulung sollte auch eine realistische Selbsteinschätzung fördern. Die Anwendenden sollten erkennen, wann Experten hinzugezogen werden sollten.

1.2.2 Meldung von Sicherheitsproblemen

Verantwortlich für Initiierung: Key-User

Verantwortlich für Umsetzung: IT-Verantwortliche

Auftretende Sicherheitsprobleme aller Art (Systemabstürze, fehlerhaftes Verhalten von bisher fehlerfrei laufenden Anwendungen, Hardwareausfälle, Eindringen Unbefugter, Manipulationen, Virenbefall u. a.) sind dem zuständigen Key-User mitzuteilen. Jeder schwerwiegende Vorfall ist zu dokumentieren (z.B. durch einen Screenshot) und der zuständigen Abteilungsleitung und der Verwaltungsleitung zu melden.

1.2.3 Konsequenzen und Sanktionen bei Sicherheitsverstößen

Verantwortlich für Initiierung: Verwaltungsleitung

Verantwortlich für Umsetzung: Verwaltungsleitung

Verstöße werden nach den geltenden rechtlichen Bestimmungen geahndet. Als Verstoß gilt die vorsätzliche oder grob fahrlässige Nichtbeachtung der IT-Sicherheitsrichtlinien und IT-Konzepte, insbesondere wenn sie

- die Sicherheit der Mitarbeitenden, Nutzer, Vertragspartner, Berater und des Vermögens der Organisation in erheblichem Umfang beeinträchtigt,
- der Organisation erheblichen finanziellen Verlust durch Kompromittierung der Sicherheit von Daten oder Geschäftsinformationen einbringt,
- den unberechtigten Zugriff auf Systeme und Informationen, deren Preisgabe und/oder Änderung beinhaltet,
- die Nutzung von Informationen der Organisation für illegale Zwecke beinhaltet und
- den unbefugten Zugriff auf personenbezogene Daten ermöglicht.

Beurteilung und Ahndung eines Verstoßes erfolgen für Mitarbeitende der Organisation in jedem Einzelfall unter Beteiligung der Mitarbeitervertretung. Zur Gefahrenintervention können entsprechend einer Organisationsrichtlinie zur IT-Sicherheit von einem IT-Beauftragten und einem internen oder externen Rechenzentrum Netzzugänge oder Benutzerkonten vorübergehend stillgelegt werden.

1.3 Sicherung der Infrastruktur

1.3.1 Räumlicher Zugangsschutz

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Personal, IT-Anwendende

Der unbefugte Zugang zu Geräten und die unbefugte Nutzung der Informationstechnik muss verhindert werden. Bei Abwesenheit sind Räume mit Informationstechnologie verschlossen zu halten. Bei der Anordnung und baulichen Einrichtung der Geräte ist darauf zu achten, dass schützenswerte Daten nicht von Unbefugten eingesehen werden können. Beim Ausdrucken derartiger Daten muss das Entnehmen der Ausdrucke durch Unbefugte verhindert werden. Geeignete Zentraldrucksysteme, gesichert durch personalisierte Codes, sollen dafür genutzt werden.

1.3.2 Sicherung mobiler Computer

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Anwendende

Bei der Speicherung von schützenswerten Daten auf mobilen Computern (Notebooks) sind besondere Vorkehrungen zum Schutz der Daten zu treffen. Die Dateien müssen verschlüsselt werden. Notebooks sind möglichst verschlossen aufzubewahren. Auf Datensicherung ist besonders Wert zu legen.

1.4 Hard- und Software

1.4.1 Kontrollierter Softwareeinsatz

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Anwendende

Auf Rechnersystemen der Organisation darf zum Zweck des Schutzes von Organisationseigener Hardware und dem Organisationsnetz nur Software installiert werden, die zur Erfüllung der dienstlichen Aufgaben erforderlich ist. Das eigenmächtige Einspielen, insbesondere auch das Herunterladen von Software aus dem Internet oder das Starten von per E-Mail erhaltener Software, ist nur gestattet, wenn sichergestellt ist, dass von dieser Software keine Gefährdung für das IT-System bzw. das Datennetz ausgeht. In jedem Fall ist vorher die Zustimmung der Abteilungsleitung der betreffenden Organisationseinheit einzuholen.

1.4.2 Keine private Hard- und Software

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Anwendende

Die Benutzung von privater Hard- und Software in Verbindung mit technischen Einrichtungen der Organisation und deren Netzen ist grundsätzlich nicht gestattet. Die Abteilungsleitung der betreffenden Organisationseinheit kann Ausnahmen gestatten. Allgemeine Ausnahmen gelten für den Einsatz von privaten Geräten nur in extra dafür bereitgestellten Gastnetzwerken.

1.4.3 Virenschutz

Verantwortlich für Initiierung: Key-User, IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Personal, IT-Anwendende

Auf allen Arbeitsplatzrechnern ist, soweit technisch möglich, ein aktueller Virenscanner einzurichten, der automatisch alle eingehenden und zu öffnenden Dateien überprüft. Damit soll bereits das Eindringen von schädlichen Programmen erkannt und verhindert werden.

Per E-Mail erhaltene Anhänge sind nur dann zu öffnen, wenn ihre Herkunft und Ungefährlichkeit sichergestellt ist. Bei Verdacht auf Vireninfektion ist unverzüglich der zuständige Key-User zu informieren.

1.5 Zugriffsschutz

1.5.1 Abmelden und ausschalten

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Personal, IT-Anwendende

Bei kürzerem Verlassen des Zimmers muss der Arbeitsplatzrechner durch einen Kennwortschutz gesperrt werden. Bei längerem Verlassen des Zimmers muss sich der Benutzer aus den laufenden Anwendungen und dem Betriebssystem abmelden. Grundsätzlich sind die Systeme nach Dienstschluss auszuschalten. Von diesen Regelungen kann nur abgewichen werden, soweit es die Arbeitsorganisation dringend erfordert und/oder andere Sicherheitsmaßnahmen es ermöglichen.

1.5.2 Personenbezogene Kennungen

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Personal, IT-Anwendende

Alle Rechnersysteme sind so einzurichten, dass nur berechtigte Benutzer die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist zunächst eine Anmeldung mit Benutzerkennung und Passwort erforderlich. Die Vergabe von Benutzerkennungen für die Arbeit an IT-Systemen soll in der Regel personenbezogen erfolgen. Die Arbeit unter der Kennung einer anderen Person ist unzulässig. Dem Benutzer ist untersagt, Kennungen und Passwörter weiterzugeben. Ausgenommen von dieser Regelung sind Systeme, die für allgemeine Zugänge bestimmt sind (z. B. Schulungsumgebungen, Empfangs- und Informationssystem).

1.5.3 Gebrauch von Passwörtern

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Personal, IT-Anwendende

Der Benutzer hat sein Passwort geheim zu halten. Idealerweise sollte das Passwort nicht notiert werden. Für die Wahl von Passwörtern werden folgende Regeln dringend empfohlen:

- Das Passwort muss mindestens 8 Stellen lang sein.
- Das Passwort darf nicht leicht zu erraten sein wie Namen, Kfz-Kennzeichen, Geburtsdaten.
- Das Passwort muss mindestens einen Groß- und Kleinbuchstaben und mindestens eine Ziffer und mindestens ein Sonderzeichen enthalten.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Das Passwort muss geheimgehalten werden und sollte nur dem Benutzer persönlich bekannt sein.
- Das Passwort ist regelmäßig, spätestens nach 360 Tagen, zu wechseln und sollte eine Mindestgültigkeitsdauer von einem Tag haben.
- Neue Passwörter müssen sich vom alten Passwort, über mehrere Wechselzyklen hinweg, signifikant unterscheiden.
- Das Passwort sollte nur für die Hinterlegung schriftlich fixiert werden, wobei es dann in einem verschlossenen Umschlag sicher aufbewahrt wird. Wird es darüber hinaus aufgeschrieben, ist das Passwort zumindest so sicher wie eine Scheckkarte oder ein Geldschein aufzubewahren.
- Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist.
- Die Eingabe des Passwortes muss unbeobachtet stattfinden.
- Auf die Einhaltung der Regeln ist insbesondere zu achten, wenn das System diese nicht erzwingt. Abweichungen von den oben genannten Regeln sollten in einer separaten Sicherheitsrichtlinie für Passwortschutz festgelegt werden.

Erhält ein Benutzer beim Anmelden mit seinem Passwort keinen Zugriff auf das System, besteht die Gefahr, dass sein Passwort durch Ausprobieren ermittelt werden sollte, um illegal Zugang zum System zu erhalten. Solche Vorfälle sind dem Abteilungsleitenden und dem IT-Personal zu melden.

Vergisst ein Benutzer sein Passwort, hat er beim Administrator ohne vorheriges Ausprobieren das Zurücksetzen zu veranlassen. Diese Festlegung soll verhindern, dass der Vorgang als Eindringversuch protokolliert und behandelt wird.

1.5.4 Zugriffsrechte

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Personal

Der Benutzer darf nur mit den Zugriffsrechten ausgestattet werden, die unmittelbar für die Erledigung seiner Aufgaben vorgesehen sind. Insbesondere sind alltägliche Arbeiten nicht mit privilegierten Benutzerkonten (Administrator, root o. a.) vorzunehmen. Bei allen administrativen Anwendungen, die gesetzlichen Anforderungen genügen müssen (Datenschutz, u. a.) erfolgt die Vergabe bzw. Änderung der Zugriffsrechte für die einzelnen Benutzer auf schriftlichen Antrag, wobei die Übersendung per E-Mail ausreichend ist. In allen anderen Bereichen sind die dort geltenden Regelungen zu beachten. Bei der Vergabe von Zugriffsrechten ist die Funktionstrennung zu beachten.

1.5.5 Netzzugänge

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Personal, IT-Anwendende

Der Anschluss von Systemen an das Datennetz der Organisation hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (Switches, Access Points, Modems o. ä.) ist unzulässig. Ausnahmen dürfen nur durch das zuständige IT-Personal in Absprache mit einem IT-Beauftragten des Bereichs und ggf. mit dem Datenschutzbeauftragten eingerichtet werden. An das Datennetz dürfen nur die dafür vorgesehenen Systeme an den vorgesehenen Stellen angeschlossen werden.

1.5.6 Telearbeit

Verantwortlich für Initiierung: Verwaltungsleitung

Verantwortlich für Umsetzung: IT-Personal, IT-Anwendende

Bei der Telearbeit verlassen Daten den räumlich eingegrenzten Bereich der Daten verarbeitenden Stelle. Zur Einrichtung und zum Betrieb von Telearbeitsplätzen ist eine individuelle Vereinbarung erforderlich (Nutzung von Hardware, Internetverbindungen, Zugangssystemen und Beachtung von Sicherheitsrichtlinien). Dabei sind die Rahmenbedingungen jedes Einzelfalls zu berücksichtigen. Der telearbeitende IT-Anwendende hat die entsprechenden Vereinbarungen zum Schutz der bearbeiteten Daten und verwendeten Systeme einzuhalten.

Telearbeit wird über die jeweilige Leitungsebene bei der Verwaltungsleitung beantragt und, nach Rücksprache mit dem zuständigen IT-Betreuer, in Bezug auf ihre Integrität zur Verfügung gestellt.

1.6 Kommunikationssicherheit

1.6.1 Sichere Netzwerknutzung

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Personal, IT-Anwendende

Der Einsatz von verschlüsselten Kommunikationsdiensten ist, nach Möglichkeit, den unverschlüsselten Diensten vorzuziehen. Die Übertragung schützenswerter Daten muss verschlüsselt erfolgen oder durch andere geeignete Maßnahmen (z. B. isolierter eigener Netze) gesichert werden.

1.7 Datensicherung

1.7.1 Datensicherung

Verantwortlich für Initiierung: IT-Verantwortliche, Key-User, IT-Anwendende

Verantwortlich für Umsetzung: IT-Personal

Regelmäßig durchgeführte Datensicherungen sollen vor Verlust durch Fehlbedienung, technische Störungen o. ä. geschützt werden. Grundsätzlich sind Daten auf zentralen Servern zu speichern. Ist die Speicherung auf zentralen Servern noch nicht möglich, ist der Benutzer für die Sicherung seiner Daten selbst verantwortlich. Bei zentraler Datensicherung sollte sich der Nutzer über die in den jeweiligen Bereichen geltenden Regelungen zu Rhythmus und Verfahrensweise für die Datensicherung informieren.

1.8 Datenträger

1.8.1 Umgang mit Datenträgern

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Personal, IT-Verantwortliche

Datenträger sind an gesicherten Orten aufzubewahren, ggf. sind Tresore zu nutzen. Weiterhin sind Datenträger zu kennzeichnen, falls die Identifikation des Datenträgers nicht durch ein anderes technisches Verfahren erfolgt. Datenträger müssen beim Transport vor Beschädigungen geschützt sein. Bei schützenswerten Daten ist eine Verschlüsselung erforderlich.

1.8.2 Weitergabe und Entsorgung von Datenträgern

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Personal, IT-Anwendende

Die Weitergabe und Entsorgung von Datenträger an nicht autorisierte Personen ist verboten. Alle Datenträger müssen zur Löschung und Entsorgung an die IT zurückgegeben werden. Auszusondernde oder defekte Datenträger müssen durch die IT vollständig unlesbar gemacht werden, sofern sie schützenswerte Daten enthalten oder enthalten haben.

1.8.3 Verlust von Hardwaregeräten und Datenträgern

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Personal, IT-Anwendende

Der Verlust von Hardwaregeräten und Datenträgern ist unverzüglich bei der jeweiligen Leitungsebene und dem zuständigen IT-Betreuer anzuzeigen.

1.9 Einsatz mobiler Geräte

Verantwortlich für Initiierung: IT-Verantwortliche,

Verantwortlich für Umsetzung: Key-User, IT-Personal, IT-Anwendende

Die Nutzung mobiler Geräte sowie die externe Datenverarbeitung werden über die jeweilige Leitungsebene bei der Verwaltungsleitung beantragt und nach Rücksprache mit dem zuständigen IT-Betreuer zur Verfügung gestellt.

- Es dürfen ausschließlich die von der Verwaltungsleitung bereitgestellten externen Datenträger auf hauseigenen Systemen, wie z.B. PCs und Notebooks verwendet werden.
- Der Einsatz und die Verwendung von hauseigenen mobilen Datenträgern auf fremden/externen Systemen oder Geräten sind nicht gestattet.
- Fremde oder private Datenträger dürfen nicht auf oder in hauseigenen Systemen und Geräten verwendet werden.
- Die Sicherheitsanforderungen für den Einsatz und die Verschlüsselung von Hard- und Software sind einzuhalten.

1.10 Schützenswerte Daten

1.10.1 Schützenswerte Daten auf dem Arbeitsplatzrechner

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Personal, IT-Anwendende

Das Speichern schützenswerter Daten auf der Festplatte des Arbeitsplatzrechners oder anderer lokaler Speicher- oder Übertragungsmedien und deren Übertragung ist nur zulässig, wenn die für den jeweiligen Schutzbedarf erforderlichen Sicherheitsmaßnahmen getroffen wurden. (Die erforderlichen Sicherheitsmaßnahmen müssen über die jeweilige Leitungsebene in Absprache mit der Verwaltungsleitung festgelegt werden).

1.10.2 Sichere Entsorgung vertraulicher Papiere

Verantwortlich für Initiierung: IT-Verantwortliche

Verantwortlich für Umsetzung: IT-Personal, IT-Anwendende

Papiere mit vertraulichem Inhalt (auch Testausdrucke) sind ordnungsgemäß zu vernichten. Alternativ kann die Entsorgung auch zentral über einen Dienstleister erfolgen. Bei der Entsorgung über einen Dienstleister sind die organisatorischen Regelungen zu beachten.

2 Konzept für einen PC-Arbeitsplatz

2.1 Sicherheitsstandards für einen PC-Arbeitsplatz

Der Evangelisch-Lutherische Kirchenkreis Lübeck-Lauenburg stellt grundsätzlich einen PC-Arbeitsplatz (Standarddesktop) zur Verfügung. Dieser besteht aus einer Microsoft Windows 10 Oberfläche mit der Bürosoftware Microsoft Office 2010. Anwendungssoftware muss sich in diesen Standarddesktop integrieren lassen. Dieses ist ein KO – Kriterium, d.h. neue Anwendungssoftware muss eine Bereitstellung in dieser Umgebung unterstützen und mit allen Komponenten kompatibel sein.

Die folgenden Komponenten und Kriterien für einen PC-Arbeitsplatz (Standarddesktop) sind zu beachten.

2.1.1 Computer Hardware

Unter Berücksichtigung von Ausfallsicherheit, Wartungskosten und Garantieansprüchen werden einheitliche Business Rechner (Sff-PC) mit möglichst identischen Hardwareserien eingesetzt. Sff-PCs haben einen geringeren Stromverbrauch gegenüber handelsüblichen PCs. Dadurch wird die Umwelt und das Klima entsprechend weniger belastet. Bezieht man noch andere Gesichtspunkte wie Produktion, Rohstoffverbrauch, Entsorgung und Transport mit ein, haben die kleinen Geräte ein noch viel größeres Einsparpotential.

2.1.2 Monitore

Zur Erfüllung der ergonomischen Anforderungen an einen Bildschirmarbeitsplatz werden höhenverstellbare Business Geräte eingesetzt, die zudem einen geringeren Energieverbrauch und eine entsprechende Kompatibilität für einen PC-Arbeitsplatz aufweisen.

2.1.3 Betriebssysteme und Softwareapplikationen

Die aktuellen Betriebssysteme und Softwareapplikationen sind unter dem Kapitel 2.2 aufgeführt.

2.1.4 Peripheriegeräte

Peripheriegeräte werden entsprechend der Arbeitsplatzanforderungen zur Verfügung gestellt. Hierzu gehören beispielsweise: Telefon, Maus und Tastatur.

2.1.5 Sonstige Hardwareausstattungen

Sonstige Hardware wird über den jeweiligen Key-User bei der Verwaltungsleitung beantragt und, nach Rücksprache mit dem IT-Zuständigen, in Bezug auf ihre Integrität zur Verfügung gestellt. Dazu zählen:

- Drucker
- Scanner
- ergonomische Mäuse, Tastaturen, etc.
- behindertengerechte Hardwarekomponenten
- Headsets
- Kartenlesegeräte
- sonstige Hardware für fachliche Aufgaben

2.1.6 Sicherheit

PC-Arbeitsplätze werden in geschlossenen/verschließbaren Räumen aufgestellt. Funkkomponenten z.B. für WLAN oder Bluetooth sind deaktiviert. Die Netzwerkanschlüsse werden über ein LAN-Kabel (Kupferkabel) hergestellt. Die Anmeldung und Authentifizierung an einem Arbeitsplatz-PC ist nur über einen personifizierten Benutzer möglich. Zum Schutz vor Schadsoftware werden automatisch aktualisierte Softwarelösungen eingesetzt. Des weiteren wird eine Verschlüsselungssoftware für Dateien bereitgestellt.

3 Software

3.1 Betriebssysteme

- Microsoft Windows 7 Prof. 64-Bit
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 R2

3.2 Standardsoftware

Standardsoftware wird für alle Arbeitsplatz-PCs definiert (siehe nachfolgende Liste).

- Microsoft Office 2010
- Adobe Reader DC
- Adobe Flash Player
- Adobe AIR
- Silverlight
- 7-Zip (Verschlüsselungssoftware)
- Sophos Virenschutz
- Citrix Receiver
- FreePDF
- GPL Ghostscript
- JAVA
- Notepad++
- VLC MediaPlayer
- Mozilla Firefox
- ActivaTSP (TAPI)
- WinPrint Hylafax
- HumanConcepts OrgPlus Reader
- irfanview

3.3 Spezielle Fachsoftware

Spezielle Fachsoftware wird über die jeweilige Leitungsebene bei der Verwaltungsleitung beantragt und nach Rücksprache mit dem IT-Zuständigen in Bezug auf ihre Integrität zur Verfügung gestellt (siehe nachfolgende Liste). Für die einzelnen Fachanwendungen werden Applikationssteckbriefe durch die jeweilige Fachabteilung erstellt und gepflegt.

Zum Beispiel: Cobra P:\Cobra\Info\Cobra_Applikationssteckbrief.xlsx

Spezielle Fachsoftware

- Cobra
- SFirm
- Archikart
- Augias
- Compuarchiv
- pcBAT TVÖD
- pcLohnsteuer
- Elsterformular
- ELV (Zeiterfassung)
- ECKD-Portal
- PORTAL (Hewlett Packard)
- steuerXpert (NWB)
- PC-Gehalt
- RehaDAT
- SV.Net
- InterWatt
- DIVA
- KIDICAP
- KirA
- Navision Web Portal (Citrix ECKD)
- Navision Web-Client (Citrix ECKD)
- RNBKita
- RNBOffice
- OpenOffice
- E-POSTBUSINESS BOX
- Maperitive
- Josm
- Osmconvert
- Joomla
- Perl Package Manager
- TOR
- WinSCP
- HARDCOPY
- OpenStreetMap
- Adobe Photoshop
- Blow_up_Photoshop
- BlueControl - Winkhaus
- DWG-Viewer
- PDFCreator

4 Berechtigungskonzept

4.1 Benutzerkonten- und Rechteverwaltung

Die Authentifizierung einzelner Benutzer im Active Directory dient im Wesentlichen dazu, differenzierte Zugriffsrechte auf Dateien, Applikationen, Geräte oder Funktionen vergeben zu können. Diese Zugriffsrechte sollten aber niemals direkt an einzelne Benutzer bzw. deren Konten im Active Directory vergeben werden. Diese Art der Rechteverwaltung würde einen immensen Aufwand erforderlich machen, wenn neue Mitarbeitenden in die Verwaltung eintreten oder auch nur innerhalb der Organisation einen anderen Aufgabenbereich umgesetzt werden.

Stattdessen werden jedem Mitarbeitenden eine (oder auch mehrere) sogenannte Rollen wie z.B. „Mitarbeitende Meldewesen" und „Mitarbeitendenvertretung" zugeordnet. Jede Rolle wird im Active Directory repräsentiert durch eine Benutzergruppe. Die für die Rolle notwendigen Zugriffsrechte auf Dateien, Applikationen etc. werden dann (einmalig) der entsprechenden Benutzergruppe gegeben. Umbesetzungen der Mitarbeitenden können dann ausschließlich über Veränderungen in den Mitgliedschaften der Benutzergruppen abgebildet werden, was eine deutliche Vereinfachung in der Administration darstellt.

4.2 Beantragung und Einrichtung von Zugriffsrechten

Die Einrichtung und Vergabe von Zugriffsrechten wird durch die jeweilige Leitungsebene bei der Verwaltungsleitung beantragt. Der dazu benötigte Prozess wird durch die zuständige Leitung und den entsprechenden verfahrensverantwortlichen Personen erarbeitet. Darin ist die Beauftragung zum Anlegen, Erstellen, Umziehen, Löschen, Freigeben und Pflegen von Zugriffrechten festzulegen.