Ordnung zur Sicherstellung der Anforderungen an den Datenschutz in der Informationstechnik (IT) (IT-Sicherheitsordnung)

Vom 8. Juli 2013 (ABl. Anhalt 2013 Bd. 1, S 3); Zustimmung der Landessynode durch Beschluss vom 14.11.2013 (ABl. Anhalt 2013 Bd. 2, S. 38); zuletzt geändert durch Kirchengesetz vom 21. April 2015 (ABl. Anhalt 2015 Bd. 1 S. 2)

Die Kirchenleitung hat nach Maßgabe des gemäß § 59 Absatz 1 Buchstabe b Kirchenverfassung auf Grund von § 9 Absatz 2 Satz 2 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland vom 12.11.1993 (ABl. EKD S. 505) in der Fassung der Neubekanntmachung vom 1.1.2013 (ABl. EKD 2013 S. 2 und S. 34) die folgende gesetzesvertretende Verordnung beschlossen:

Inhaltsverzeichnis

Präambel	2
§ 1 Geltungsbereich	2
§ 2 IT-Sicherheitsstandard	2
§ 3 IT-Sicherheitsziele	3
§ 4 Voraussetzungen für den Einsatz von Informationstechnik	3
§ 5 Nutzung von IT-Geräten	4
§ 6 Schulungs- und Fortbildungsmöglichkeiten	4
§ 7 IT-Sicherheitsbeauftragter	4
§ 8 Einhaltung der IT-Sicherheit	5
§ 9 Ausführungsbestimmungen	5
§ 10 Inkrafttreten	5

Präambel. [1]Der Gebrauch von Computern und Netzen ist für die haupt-, neben- und ehrenamtlichen Mitarbeitenden in der Evangelischen Landeskirche Anhalts zur alltäglichen Routine geworden. [2]Bei ordnungsgemäßer Benutzung erleichtert der Computer viele Tätigkeiten und manche Arbeiten wären ohne den Einsatz von Computern gar nicht mehr denkbar. [3]Fahrlässige oder gar gesetzwidrige Verwendung hingegen kann die Rechte anderer verletzen. [4]Daher haben alle Nutzer sorgfältig und verantwortungsvoll unter Einhaltung der rechtlichen Vorschriften Computer und Netze zu nutzen.

[5]In dieser Vorschrift wird aufgezeigt, welche Mindeststandards für den Betrieb eines Computers bzw. eines Netzes verbindlich sind und welche Konsequenzen bei Nichteinhaltung der IT-Sicherheitsordnung gezogen werden. [6]Zweck der IT-Sicherheitsordnung ist es, diese Themenkreise zu formalisieren und allen Benutzern eine einheitliche Grundlage zu bieten, anhand derer entschieden werden kann, welche Benutzung konform ist und welche Maßnahmen zu ergreifen sind.

[7]Die Informationssicherheit ist systematisch und umfassend an die technischen und rechtlichen Entwicklungen anzupassen, damit eine möglichst optimale Sicherheitsfunktionalität bei vertretbaren Kosten erreicht wird. [8]Dabei sind die umgesetzten Lösungen praxistauglich und ausreichend komfortabel zu gestalten, damit sie

von den Mitarbeitenden auch in der täglichen Arbeit nicht als belastend, sondern als sinnvoll akzeptiert werden.

[9] Auf Grund einer maximalen Offenheit kann Missbrauch a priori nicht ausgeschlossen werden. [10] Durch die IT-Sicherheitsordnung soll für IT-Sicherheit sensibilisiert werden. [11] Die IT-Sicherheitsordnung soll als Richtschnur für das eigene Handeln sowie für das Beurteilen des Handelns der Anderen dienen.

§ 1 Geltungsbereich. Die IT- Sicherheitsordnung ist verbindlich für sämtliche haupt-, neben- und ehrenamtlich Mitarbeitenden in der Evangelischen Landeskirche Anhalts sowie für Dritte, mit denen die Benutzung von Computern und Netzen von kirchlichen Einrichtungen vereinbart worden ist.

§ 2 IT-Sicherheitsstandard. (1) Die mit der Informationstechnik (IT) erhobenen und verarbeiteten Daten sind insbesondere vor unberechtigtem Zugriff, vor unerlaubten Änderungen und vor der Gefahr des Verlustes zu schützen (IT-Sicherheit), um deren Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

(2) [1] Jede kirchliche Stelle im Sinne des § 1 Absatz 2 Satz 1 des Datenschutzgesetzes der EKD (DSG-EKD) hat das vom Landeskirchenrat erstellte aktuelle ITSicherheitskonzept der Landeskirche umzusetzen. [2] Der Landeskirchenrat hat das IT-Sicherheitskonzept regelmäßig zu aktualisieren.

(3) [1] Bei der Erstellung und der regelmäßigen Fortschreibung des IT-Sicherheitskonzeptes und bei der Entscheidung zur Auswahl über IT, mit der personenbezogene Daten verarbeitet werden, ist – soweit vorhanden – der Betriebsbeauftragte für den Datenschutz frühzeitig zu beteiligen. [2] Anderenfalls ist der landeskirchliche Beauftragte nach § 18 DSG-EKD zu beteiligen.

(4) [1] Der für die Umsetzung des IT-Sicherheitskonzeptes erforderliche Sicherheitsstandard orientiert sich an den jeweiligen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Informationssicherheit und zum IT-Grundschutz oder einem vergleichbaren Standard. [2] Das IT-Sicherheitskonzept muss geeignete Maßnahmen gegen Gefährdungen von innen und außen enthalten. [3] Die IT-Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zum Schutzbedarf der Daten und der ITSysteme stehen.

(5) [1] Die Evangelische Landeskirche Anhalts führt für ihren Bereich eine Übersicht über die kirchlichen Werke und Einrichtungen mit eigener Rechtspersönlichkeit, für die das DSG-EKD gilt (gemäß § 1 Absatz 2 Sätze 3 und 4 DSG-EKD). [2] Der Landeskirchenrat stellt Muster-IT-Sicherheitskonzepte insbesondere für die Landeskirche, die Kirchengemeinden und die im Satz 1 erwähnten Werke und Einrichtungen zur Verfügung, die die Mindestanforderungen der IT-Sicherheit unter Berücksichtigung der örtlichen und sachlichen Gegebenheiten darstellen und die einzuhalten sind.

§ 3 IT-Sicherheitsziele. (1) Die IT-Sicherheitsordnung definiert grundlegende Ziele einer IT-Sicherheit und legt Verantwortlichkeiten sowie Rahmenbedingungen für die Umsetzung der IT-Sicherheitsstandards fest.

(2) Die mit der Informationstechnik erhobenen, verarbeiteten und genutzten Daten sind zu schützen, insbesondere im Hinblick auf

a) deren Zugänglichkeit/Verfügbarkeit. Daten und Anwendungen müssen dem jeweiligen Nutzungsprofil entsprechend jederzeit an den dafür eingerichteten Arbeitsplätzen verfügbar sein. Voraussetzung für die Aufrechterhaltung der Datenverfügbarkeit ist die Sicherung aller IT-

Komponenten und der technischen und räumlichen Infrastruktur gegen organisationsbedingte, technische und umweltbedingte Ausfälle. Zentrale, aber auch dezentrale IT-Systeme müssen funktionieren, um die Verfügbarkeit der Daten zu garantieren.

b) deren Integrität. Daten und Anwendungen dürfen nicht unberechtigt gelöscht, zerstört oder manipuliert werden.

c) den Schutz der Daten vor Verlust. Der Verlust der Daten ist durch geeignete Maßnahmen zu verhindern.

d) der Vertraulichkeit. Daten und Anwendungen dürfen grundsätzlich nur von Personen gelesen und benutzt werden, die dazu eine Zugriffsberechtigung besitzen. Die Festlegung der Zugriffsberechtigung und des erforderlichen Kontrollumfangs obliegt dem jeweiligen Verfügungsberechtigen.

e) die Einführung, Auswahl, Gestaltung und Änderung von Verfahren. In die Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten ist der gemäß § 2 Absatz 3 Zuständige rechtzeitig einzubinden. Gleiches gilt für die Neueinführung und Änderung der Verfahren.

§ 4 Voraussetzungen für den Einsatz von Informationstechnik. (1) Wesentliche Entscheidungen auf dem Gebiet der IT sind vor allem:

a) der Aufbau neuer IT-Infrastrukturen,

b) der Einsatz von Betriebssystemen,

c) der Einsatz von Anwendungsprogrammen,

d) der Einsatz freigabepflichtiger Anwendungsprogramme,

e) die Nutzung von Kommunikationstechnik.

(2) Mindestvoraussetzungen für den Einsatz von IT sind, dass

a) ein Anforderungsprofil und eine Dokumentation vorliegen,

b) die datenschutzrechtlichen Voraussetzungen eingehalten werden,

c) die Systeme vor ihrem Einsatz getestet wurden und

d) die erforderlichen Lizenzen vorhanden sind.

(3) Für den dienstlichen Datenaustausch ist der Einsatz von einheitlicher Software und IT-Strukturen in vergleichbaren Einsatzbereichen anzustreben.

(4) Bei Anwendungsprogrammen, mit denen personenbezogene Daten erhoben, verarbeitet und genutzt werden, bestehen keine datenschutzrechtlichen Bedenken, wenn

a) dies unter Berücksichtigung des Grundsatzes der Datenvermeidung und Datensparsamkeit festgestellt wird,

b) die Rechte Betroffener auf Auskunft, Berichtigung, Löschung und Sperrung ihrer personenbezogener Daten nach Maßgabe des DSG-EKD gewährleistet sind,

c) sie nach dem EKD-Recht (§§ 21 und 21a DSGEKD) freigegeben worden sind,

d) erforderliche technische und organisatorische Datenschutzmaßnahmen unter Berücksichtigung des IT-Sicherheitskonzeptes, des Schutzbedarfs und der Anforderungen der Anlage zu § 9 Absatz 1 DSG-EKD vorliegen.

§ 5 Nutzung von IT-Geräten. (1) Für die mit der IT verarbeiteten Daten sind dienstliche IT-Geräte zu nutzen, die einheitlichen Standards entsprechen.

(2) In Ausnahmefällen kann der Landeskirchenrat private Geräte zur Nutzung zulassen, wenn durch Vereinbarung insbesondere sichergestellt ist, dass

a) eine Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten vorhanden ist,

b) das kirchliche Datenschutzrecht Anwendung findet,

c) technische und organisatorische Maßnahmen zur IT-Sicherheit und zum Datenschutz vorhanden sind,

d) ein regelmäßiger und insbesondere aktueller Schutz vor Viren und anderen Schadprogrammen gewährleistet ist,

e) die Haftung ausgeschlossen wird, wenn in Zusammenhang mit dienstlichen Anwendungen Schäden auf privaten IT-Geräten, insbesondere Datenverlust, entstehen.

(3) Über die Nutzung von dienstlichen und privaten Geräten, die für dienstliche Zwecke genutzt und auf denen personenbezogene Daten gespeichert werden, führt der Landeskirchenrat ein Verzeichnis.

(4) Die Zulassung privater Geräte zur Nutzung ist zu widerrufen, wenn ein Verstoß gegen Absatz 2 festgestellt oder die IT-Sicherheit durch den Einsatz privater IT-Geräte gefährdet oder beeinträchtigt wird.

§ 6 Schulungs- und Fortbildungsmöglichkeiten. In der Landeskirche sind angemessene Schulungsund Fortbildungsmöglichkeiten für den qualifizierten Umgang mit den Anwendungsprogrammen zu ermöglichen, die zentral von der Landeskirche vorgegeben werden.

§ 7 IT-Sicherheitsbeauftragter. (1) Zur Wahrnehmung der IT-Sicherheit hat der Landeskirchenrat einen für die gesamte Landeskirche zuständigen IT-Sicherheitsbeauftragten und dessen Stellvertretenden zu bestellen.

(2) Zu Beauftragten dürfen nur Personen bestellt werden, die zur Erfüllung ihrer Aufgaben die erforderliche Fachkunde und Zuverlässigkeit besitzen.

(3) Zu den Aufgaben des IT-Sicherheitsbeauftragten gehört es insbesondere:

a) bei den den IT-Sicherheitsprozess betreffenden Aufgaben mitzuwirken,

b) die Erstellung und Fortschreibung eines IT-Sicherheitskonzeptes zu koordinieren,

c) Regelungen zur IT-Sicherheit vorzuschlagen,

d) die Realisierung von Sicherheitsmaßnahmen zu empfehlen und zu überprüfen,

e) IT-Sicherheitsvorfälle zu untersuchen und Handlungsempfehlungen auszusprechen,

f) IT-Schulungsmaßnahmen zu initiieren und zu koordinieren,

g) dem Leitungsorgan der kirchlichen Stelle auf Anforderung über den Stand der IT- Sicherheit zu berichten,

h) mit den Betriebsbeauftragten für den Datenschutz zusammenzuarbeiten.

(3) [1]Der IT-Sicherheitsbeauftragte ist unverzüglich über IT-Sicherheitsvorfälle zu informieren. [2]Dieser informiert bei Gefahr im Verzug unverzüglich das zuständige Leitungsorgan und den Beauftragten für Datenschutz. [3]Ist der IT-Sicherheitsbeauftragte nicht erreichbar, ist unverzüglich der Stellvertretende zu informieren.

§ 8 Einhaltung der IT-Sicherheit. (1) [1]Der Landeskirchenrat ist für die Einhaltung der IT-Sicherheit einschließlich der Umsetzung des ITSicherheitskonzeptes auf landeskirchlicher sowie auf kirchenkreislicher Ebene verantwortlich. [2]Der Gemeindekirchenrat ist für die Umsetzung auf kirchengemeindlicher Ebene verantwortlich, das Leitungsorgan der weiteren kirchlichen Dienststelle jeweils für deren Bereich.

(2) Die aufsichtsführenden Stellen oder Personen überwachen die Einhaltung der IT-Sicherheit. Hierfür kann der IT-Sicherheitsbeauftragte beauftragt werden.

(3) [1]Bei Verstößen gegen die IT-Sicherheit sind geeignete Maßnahmen und gegebenenfalls Regelungen zur Gefahrenintervention zu ergreifen. [2]Neben den arbeitsrechtlichen und datenschutzrechtlichen Konsequenzen sind folgende Sanktionen möglich:

1. die Beanstandung bei geringfügigen individuellen Verstößen,
2. die Aufforderung an die Leitung der Einrichtung, den Missstand unter Wahrung einer Frist zu beseitigen,
3. bei Zuwiderhandlung oder Nichteinhaltung der Frist nach Nummer 2 die Mitteilung an die Aufsichtsbehörde, im Wege der Aufsicht die Beseitigung des Missstandes anzuordnen,
4. die vorübergehende Sperrung der Zugangsberechtigung zur Datenverarbeitungsanlage, bis der Nachweis über die die Beseitigung des Missstandes erbracht ist,
5. Entzug der IT-relevanten Tätigkeit bei Ehrenamtlichen.

(4) Maßnahmen der oder des Beauftragten für Datenschutz nach § 20 DSG-EKD bleiben unberührt.

§ 9 Ausführungsbestimmungen. Der Landeskirchenrat kann Durchführungsbestimmungen beschließen.

§ 10 Inkrafttreten. Diese Regelungen treten am 1. August 2013 in Kraft.

Anlage 1: Regeln für den Umgang mit IT-Systemen und IT-Komponenten

1. Benutzen Sie nur solche IT-Systeme (z. B. PC, Laptop) und IT-Komponenten (z. B. USB-Stick oder Software), die für Ihren Arbeitsplatz vorgesehen sind.

2. Benutzen Sie dienstliche IT-Systeme nicht für persönliche Zwecke.

3. Greifen Sie nur auf Informationen zu, wenn Sie wissen, dass Sie dazu befugt sind.

4. Verändern Sie Informationen auf IT-Systemen nur, wenn Sie wissen, dass Sie dazu befugt sind.

5. [1] Führen Sie regelmäßig Datensicherungen durch. [2] Bewahren Sie die Datenträger so auf, dass sie vor unberechtigtem Zugriff geschützt sind. [3] Sofern dienstliche Daten auf lokalen IT-Systemen gespeichert werden, sind diese Daten zu verschlüsseln.

6. Sorgen Sie für einen aktuellen Virenschutz auf Ihrem IT-System und nutzen diesen regelmäßig, denn Internetzugänge sind durch geeignete Maßnahmen (Router, Firewall, Virenscanner) zu schützen.

7. Informieren Sie sich regelmäßig, wie Sie sich als Benutzer zu verhalten haben, wenn der Verdacht besteht, dass IT-Sicherheit gefährdet ist (z.B. unberechtigter Zugriff, Datenverlust, Computervirus).

8. Benutzen Sie keine Passwörter von anderen Personen.

9. [1] Halten Sie Ihre Passwörter vertraulich. [2] Wenn Sie um Ihr Passwort gebeten werden, verweisen Sie an den zuständigen Administrator. [3] Wenn für die IT-Unterstützung Ihr Passwort benötigt wird, sollten Sie das Passwort selbst eingeben und die durchzuführenden Arbeiten beaufsichtigen. [4] Denken Sie daran: Sie sind für alles verantwortlich, was unter Ihrem Benutzernamen und Ihrem Passwort passiert.

Anlage 2: IT-Sicherheitskonzept

1. Bedeutung der Informationstechnologie (IT). Informationstechnologie ist ein Instrument zur Erfüllung von wichtigen Aufgaben und zur Unterstützung von Funktionen auf allen Ebenen der Evangelischen Landeskirche Anhalts.

2. Schutz der IT-Systeme und dienstlichen Daten. [1] IT-Systeme und dienstliche Daten sind vor unberechtigtem Zugriff und vor unerlaubter Änderung zu schützen (IT-Sicherheit). [2] Jede kirchliche Körperschaft ist verpflichtet, IT-Sicherheit zu gewährleisten. [3] Dafür die das jeweilige Leitungsorgan verantwortlich.

3. IT-Sicherheitsziele. [1] Die Daten und IT-Systeme werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können. [2] Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (Integrität). [3] Die Anforderungen an Vertraulichkeit haben ein normales, an Gesetzeskonformität orientiertes Niveau. [4] Zur Erreichung dieser IT-Sicherheitsziele ist jede kirchliche Körperschaft verpflichtet, IT-Sicherheit zu organisieren. [5] In den Bereichen, in denen Programme mit schutzbedürftigen Daten eingesetzt werden, insbesondere Meldewesen, Kirchenbuchwesen, Personalwesen, Haushalts-, Kassen- und Rechnungswesen, sind die IT-Sicherheitsziele (Verfügbarkeit, Integrität und Vertraulichkeit) mit Priorität zu beachten.

4. E-Mail-System. [1] Die Nutzung des landeskirchlichen E-Mail-Systems dient zur dienstlichen Kommunikation. [2] Entsprechende Maßnahmen stellen sicher, dass die Risiken gering bleiben. [3] Die gesetzlichen Regelungen sind zu beachten. [4] Materielle und immaterielle Folgen durch Gesetzesverstöße sowie die Verursachung sonstiger Schäden müssen verhindert werden.

5. IT-Sicherheitsmanagement. [1] Die im IT-Sicherheitskonzept definierten Sicherheitsmaßnahmen, insbesondere Maßnahmen gegen die Bedrohungen von innen und außen, müssen umgesetzt werden. [2] Diese Umsetzungwird regelmäßig überprüft. [3] Wenn dienstliche Daten an außerkirchliche Stellen weitergeleitet werden müssen, ist eine größtmögliche Datensicherheit zu gewährleisten. [4] Daneben sind über die Erfordernisse des Datenschutzes hinaus alle dienstlichen Daten in geschützten Bereichen zu speichern. [5] Der Zugang zu zentralen Servern und Netzwerkkomponenten soll durch ausreichende Zugangskontrollen geschützt werden. [6] Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen gewährleistet. [7] Der Zugriff auf die Daten wird durch ein restriktives Berechtigungskonzept geschützt. [8] Jede kirchliche Körperschaft sorgt dafür, dass ihr internes Netz durch eine geeignete Firewall gesichert wird. [9] IT-Benutzer informieren bei Störfällen das Landeskirchenamt oder den IT-Sicherheitsbeauftragten. [10] IT-Benutzer sollen über die Gefahren im Umgang mit IT regelmäßig informiert werden. [11] Für eine angemessene Datensicherung müssen Regelungen getroffen werden.

Erläuterungen zur IT-Sicherheitsordnung

1. Informationstechnologie

Informationstechnologie (IT) ist ein Instrument zur Erfüllung von wichtigen Aufgaben und zur Unterstützung von Funktionen auf allen Ebenen der Evangelischen Kirche und ihrer Diakonie. IT-Sicherheit stellt einen Teil der Informationssicherheit dar. Jede kirchliche und jede diakonische Stelle (die Legaldefinition enthält in § 1 Absatz 2 Satz 1 EKD-Datenschutzgesetz) ist gemäß § 9 Absatz 2 EKD-Datenschutzgesetz verpflichtet, IT-Sicherheit zu gewährleisten.

Das EKD-DSG gilt in der gesamten EKD. Es ist unter: http://www.kirchenrecht-ekd.de/showdocument/id/25764/orga_id/EKD/search/EKD-Datenschutzgesetz) einsehbar.

Durch bestehende Risiken der Informationstechnologie wird ein Handlungsdruck erzeugt.

Bei Nichtbeachtung und Vernachlässigung dieser Risiken besteht die Gefahr massiver Reputations- oder wirtschaftlicher Schäden über die jeweilige kirchliche Stelle hinaus. Sicherheitsvorfälle können nur durch ein aktives Handlungsmanagement verhindert werden.

Die Zuständigkeit hierfür geht über die jeweilige IT-Fachabteilung hinaus und bezieht alle handelnden Personen, Akteure und Dienststellen im Rahmen ihrer Tätigkeit mit ein.

IT-Sicherheit ist eine Aufgabe hoher Priorität, für die die Kirche Sorge zu tragen hat.

2.Zielsetzung

§ 9 Absatz 1 EKD-Datenschutzgesetz verpflichtet alle kirchlichen Stellen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um insbesondere die in der Anlage zu diesem § 9 genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen, deren Aufwände in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen.

IT-Sicherheit definiert sich über drei Schutzziele, nämlich Vertraulichkeit, Integrität und Verfügbarkeit, die sich beispielhaft wie folgt darstellen:

Die Daten und IT-Systeme müssen in ihrer Verfügbarkeit so gesichert werden, dass eintretende Stillstandzeiten toleriert werden können.

Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (Integrität).

Die Anforderungen an Vertraulichkeit leiten sich vom Rechte- und Rollenkonzept des jeweiligen Datenverarbeitungssystems ab und definiert dadurch, wer auf welche Daten zugreifen darf.

In den Bereichen, in denen Programme mit zum Teil hochsensiblen schutzbedürftigen Daten eingesetzt werden, insbesondere Melde-, Kirchenbuch-, Personalwesen, Haushalts-, Kassen- und Rechnungswesen, Gesundheitsdaten, Patientenbetreuung und -verwaltung, werden an die IT-Sicherheitsziele (Verfügbarkeit, Integrität und Vertraulichkeit) besonders hohe Anforderungen zu stellen sein.

Es ist oft schwierig, ein angemessenes Sicherheitsniveau zu erreichen und aufrecht zu erhalten. Die Gründe dafür sind oft fehlende finanzielle und personelle Ressourcen, steigende Komplexität der IT-Systeme. Analog zur Entwicklung in der Informationstechnik sind die Anforderungen an IT-Sicherheit stets komplexer geworden. Eine Vielzahl von IT-Sicherheitsprodukten und -beratern bieten unterschiedlichste Lösungen an.

Auch bei den Sicherheitsprüfungen vor Ort kann es nicht nur um die einzelnen IT-Komponenten mit mehr oder weniger abgeschlossenen Maßnahmenpaketen gehen, sondern es ist ein abgeschlossenes, auf die Gegebenheiten vor Ort abgestimmtes, IT-Sicherheitskonzept für die jeweilige kirchliche Stelle entscheidend. Dabei sollte aus Gründen der Gleichwertig- und Vergleichbarkeit auf die im staatlichen Bereich zu Grunde gelegten Standards zurückgegriffen werden. IT-Sicherheit ist kein statischer Zustand, sondern ein ständiger Prozess.

3.Problemlagen

Es ist eine zum Teil weit verbreitete Fehleinschätzung anzunehmen im Hinblick auf die Notwendigkeit des eigenen Schutzbedarfs. Die Aussage „Bei uns ist noch nie etwas passiert“ kann nicht dazu führen, auf den Schutz zu verzichten. Die Einschätzung „Was soll bei uns schon zu holen sein, so geheim sind unsere Daten nicht“ ist im kirchlichen Bereich – insbesondere im Hinblick auf das kirchliche Meldewesen - nicht zutreffend. Auch die Aussage „Unsere Mitarbeiter unterliegen dem Datenschutz und sind vertrauenswürdig“ ist zwar grundsätzlich richtig, doch dient die IT-Sicherheitsordnung u.a. auch dazu, Problembewusstsein herbeizuführen. Für die kirchlichen und diakonischen Stellen sind immer wieder die folgenden Fragen zu beantworten:

- Welche Formen von Missbrauch sind denkbar, wenn vertrauliche Informationen in die Hände unbefugter Dritter gelangen? (Vertraulichkeit)
- Welche Konsequenzen sind denkbar, wenn Informationen unbemerkt verändert werden? Als Ursache kann nicht nur böse Absicht unbekannter Dritter, sondern auch technisches Versagen in Frage kommen. (Integrität)
- Welche Auswirkungen sind denkbar, wenn der Zugriff auf Computer oder andere IT-Komponenten für einen längeren Zeitraum (Tage, Wochen, ...) nicht mehr möglich ist? Könnte die Arbeit fortgesetzt werden? Wie hoch wäre der mögliche Schaden? (Verfügbarkeit)

In einem qualifizierten IT-Sicherheitskonzept sind auf diese Fragen entsprechende Lösungsansätze zu finden.

4.BSI-Standard als Grundausrichtung

Hinsichtlich dieser Grundausrichtung und zur Gewährung der Gleichwertig- und der Vergleichbarkeit eines IT-Sicherheitskonzeptes mit den staatlichen Stellen hat sich die Landeskirche an den Empfehlungen des Bundesamtes für Sicherheit und Informationstechnik (BSI) zur Informationssicherheit und zum IT-Grundschutz zu orientieren.

Dies sorgt zudem für eine anerkannte Basis. Das BSI bietet seit vielen Jahren Informationen und Hilfestellungen rund um das Thema IT-Sicherheit: Als ganzheitliches Konzept für IT-Sicherheit hat sich das Vorgehen nach IT-Grundschutz zusammen mit den IT-Grundschutz-Katalogen des BSI als Standard etabliert. Diese vom BSI seit 1994 eingeführte und weiterentwickelte Methode bietet sowohl eine Vorgehensweise für den Aufbau einer Sicherheitsorganisation als auch eine um-fassende Basis für die Risikobewertung, die Überprüfung des vorhandenen IT-Sicherheitsniveaus und die Implementierung der

angemessenen IT-Sicherheit. Die IT-Grundschutz-Kataloge dienen außerdem zahlreichen Unternehmen und staatlichen Behörden als wichtiges Fundament eigener Maßnahmenkataloge. Hierbei findet Beachtung, dass die IT-Sicherheitsmaßnahmen in einem angemessenen Verhältnis zum Wert der schützenswerten Daten und IT-Systeme stehen müssen.

5.Verantwortung und Umsetzung

Die Verantwortung für die IT-Sicherheit obliegt dem Leitungsorgan der jeweiligen kirchlichen Stelle.

Die Umsetzung ist von einem IT-Sicherheitsbeauftragten zu überwachen.

Das einheitliche IT-Sicherheitskonzept hat neben dem Sicherheitsgewinn häufig weitere Vorteile:

- Wartungsarbeiten an IT-Systemen erfordern deutlich weniger Zeit und die IT-Administratoren können effektiver arbeiten. Die IT-Systeme sind gut dokumentiert, was Administrationsarbeiten, Planung, Neuinstallation von Software und Fehlerbeseitigung erleichtert. Ein IT-Sicherheitskonzept vermeidet zudem die Fehlerbeseitigung.
- Das IT-Sicherheitskonzept stellt den Handlungsrahmen dafür zur Verfügung, dass Anwender die gleichen Programme für den gleichen Zweck einsetzen, nicht unterschiedliche Betriebssysteme betreut werden müssen, möglichst nicht verschiedene Versionen der gleichen Software im Einsatz sind und trägt im Hinblick auf die Regelungen dafür Sorge, dass Anwender nicht private Software nützen.