ARBEITSGRUPPE ZUR BEREITSTELLUNG VON MUSTER IT-SICHERHEITSKONZEPTEN

Ergebnisbericht

1 ERGEBNISZUSAMMENFASSUNG

1.1 Ausgangslage

Die Evangelische Kirche in Deutschland (EKD) mit ihren kirchlichen und diakonischen Einrichtungen verfügt in verschiedenen Bereichen über eine Vielzahl schützenswerter Daten, die zu einem beträchtlichen Teil auch eines hohen Schutzbedarfes bedürfen.

In der Vergangenheit hat sich die Evangelische Kirche bereits vielfach mit dem Schutz dieser Daten beschäftigt. Die Erkenntnisse sind in die auf der Synode 2012 der EKD verabschiedete Novellierung des Datenschutzgesetzes der EKD (DSG-EKD) eingeflossen. Diese ist seit dem 1. Januar 2013 in Kraft.

Mit dieser Novellierung wurde erstmals für alle kirchlichen Stellen die Verpflichtung zur Einhaltung der IT-Sicherheit festgelegt und normiert. Das DSG-EKD gilt unmittelbar für alle Gliedkirchen und teilweise, je nach deren Organisationsform, auch für die Werke und Einrichtungen der Diakonie. Bestandteil dieser Regelung ist es, dass für jede kirchliche Stelle ein IT-Sicherheitskonzept vorhanden sein muss. Zur Unterstützung dieses Prozesses stellt die EKD Muster-IT-Sicherheitskonzepte zur Verfügung.

Die nähere Ausgestaltung wird in einer Rechtsverordnung festgelegt, deren derzeit vorliegender abgestimmter Entwurf von der EKD unter Beteiligung gliedkirchlicher und diakonischer Vertreter unterschiedlicher Bereiche ausgearbeitet wurde. Die Muster-IT-Sicherheitskonzepte werden Bestandteil der Ratsverordnung, die im Jahr 2015 verabschiedet werden soll. Die Einhaltung dieser Zeitvorgaben geht einher mit der zurzeit erarbeiteten Erweiterung des kommunalen Datenaustausches im kirchlichen Meldewesen um das Modul Staat/Kirche (OSCI-XMeld-Verfahren). Die Aufnahme der Kirchen in dieses sichere und verlässliche Datenaustauschverfahren erfordert eine entsprechende kirchliche Regelung. Diese soll mit der Verordnung zur IT-Sicherheit geschaffen werden und baldmöglichst in Kraft treten.

In der Diakonie prüfen Wirtschaftsprüfer bereits im Rahmen der Jahresabschlussprüfung die IT-Systeme.

1.2 Vorgehensweise zur Entwicklung der Muster-IT-Sicherheitskonzepte

Die Mindestanforderungen der Muster-IT-Sicherheitskonzepte sind entsprechend der Ratsverordnung unter Berücksichtigung der örtlichen Gegebenheiten von den zuständigen kirchlichen Stellen einzuhalten. Diese sollen so rechtzeitig zur Verfügung gestellt werden, dass darauf zum Zeitpunkt der Erstellung der IT-Sicherheitskonzepte der einzelnen kirchlichen Stellen zurückgegriffen werden kann.

Für die Erarbeitung dieser Muster-IT-Sicherheitskonzepte hat das Kirchenamt der EKD eine Arbeitsgruppe gebildet. In dieser Gruppe sind neben der Kompetenz aus dem Bereichen IT und IT-Sicherheit der EKD, den Gliedkirchen und der Diakonie auch die mittlere Ebene eines Kirchenkreises sowie der Beauftragte für den Datenschutz der EKD vertreten. Die Arbeitsgruppe wird durch Vertreter der HiSolutions AG unterstützt.

Als spezialisiertes Beratungsunternehmen für Informationssicherheit und Datenschutz verfügt die HiSolutions AG über umfangreiche Erfahrungen und Experten auf diesem Gebiet. So ist die HiSolutions AG an den größten Grundschutzzertifizierungen mittels Vorbereitung oder Durchführung beteiligt gewesen. Mit der Erstellung mehrerer Standards und Bausteine für das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat das Beratungshaus den IT-Grundschutz maßgeblich mit geprägt. Es werden neun zertifizierte IT-Grundschutz-Auditoren und sechs zertifizierte IS-Revisoren beschäftigt.

Aufgrund der Heterogenität der Einrichtungen in Kirche und Diakonie werden zwei unterschiedliche Muster für kleine sowie für mittlere und große kirchliche und diakonische Einrichtungen benötigt. Für die Erarbeitung der Inhalte wurden 3 Workshops durchgeführt. Dabei wurden, die im nachfolgenden Kapitel aufgeführten und in Kapitel 2 vertiefend beschriebenen Ergebnisse diskutiert und in jeweils finale Versionen überführt.

1.3 Struktur der Ergebnisdokumente

Folgende Ergebnisdokumente sind verfügbar:

Tabelle 1: Ergebnisdokumente

Beschreibung	**Dokumentenname**
Der vorliegende übergreifende Ergebnisbericht	• Ergebnisbericht.pdf
Anlage A: Muster-IT-Sicherheitskonzept für kleine Einrichtungen	• A_Muster klein.pdf
Anlage B: Muster-IT-Sicherheitskonzept für mittlere und große Einrichtungen	• B_Muster groß.pdf
Anlage C1: Vorschläge für ein Schulungskonzept IT-Sicherheit	• C1_Schulungskonzept.pdf
Anlage C2: BfDI Musterformular: „Dienstanweisung über die Nutzung elektronischer Kommunikations-systeme am Arbeitsplatz“	• C2_Musterformular BfDI.pdf
Anlage C3: Tool-Unterstützung IT-Grundschutz	• C3_Produktvorstellung-GS-Tool-Alternativen.pdf
Anlage C4: Abgestimmte Schutzbedarfskategorien	• C4_Schutzbedarfskategorien.pdf
Anlage C5: Beispielhafte Schutzbedarfsfeststellung • Personalwesen EKD • Meldewesen EKD • Finanzwesen EKD • Patientendaten Diakonie	• C5_Schutzbedarfsfeststellung.pdf
Anlage C6: Modellierungsvorschrift der IT-Grundschutz-Kataloge zur Anwendung von Bau-steinen auf Informationsverbünde	• C6_Modellierungsvorschrift.pdf
Anlage C7: Gefährdungskatalog zur Risikoanalyse nach BSI 100-3	• C7_Gefährdungskatalog.pdf
Anlage C8: Template zur Durchführung einer Risi-koanalyse nach BSI 100-3.	• C8_Risikoanalyse-Template.pdf

Nachfolgendes Schaubild stellt die Abdeckung und die Anwendungsbereiche der Ergebnisdokumente dar.

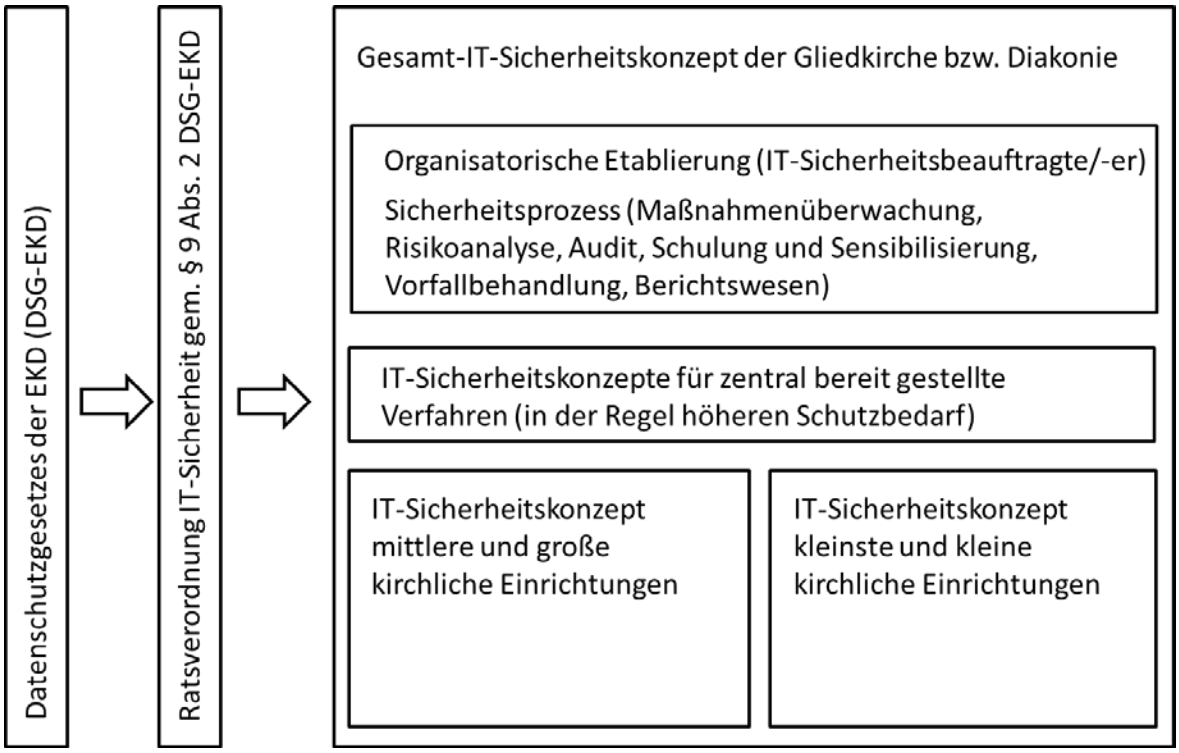

Abbildung 1: Gesamtabdeckung und Anwendung der Ergebnisdokumente

2 LEISTUNGSBESCHREIBUNG

2.1 Muster-IT-Sicherheitskonzept kleine kirchliche Einrichtungen

Bei der Ausarbeitung dieses Musters war die Anforderung, den BSI-Grundschutz mit den bei diesen Einrichtungen vorhandenen Kapazitäten umzusetzen.

Kleine Organisationen werden wie folgt definiert: kleinste und kleine Einrichtungen verfügen über kein geschultes IT-Personal, nur eine minimale Infrastruktur und eine überwiegend dezentrale Datenhaltung, z. T. zentrale Anwendungen (Melde-, Finanz- und Personalwesen). Zudem existiert z. T. keine ausreichende Abgrenzung zu privaten Bereichen (Räume und Geräte). In der Regel gibt es keine IT-Standards (Datensicherung, Kennwortregelungen) und auch keine Server.

Es ist aber unbedingt zu beachten, dass bei der Verarbeitung von Daten mit hohem und sehr hohem Schutzbedarf auch in kleinen Einrichtungen immer die Erstellung von IT-Sicherheitskonzepten gemäß dem Muster für mittlere und große Einrichtungen erforderlich ist.

Zunächst wurden auf Grund der in den BSI IT-Grundschutzkatalogen zu findenden Bausteine die relevanten Themengebiete für kleinste und kleine kirchliche Einrichtungen zusammengestellt. Danach wurde die Chance für die Anwendung vor Ort ohne das Vorhandensein sachkundigen Personals gemeinsam durch alle Anwesenden analysiert und im Ergebnis auf das Mindestmaß konsolidiert.

Ferner wurde der Vorschlag angenommen, am Ende des Muster-IT-Sicherheitskonzeptes eine Checkliste anzubieten, welche sowohl der eigenen Prüfung des Grades der Berücksichtigung aller gestellten Anforderungen vor Ort als auch, sofern in der jeweiligen kirchlichen Einrichtung gewünscht, die Möglichkeit eines minimalen Berichtswesens an die übergeordnete kirchliche Organisationseinheit bietet.

Im Ergebnis liegt ein Gesamtdokument vor, welches nach einer einleitenden Sensibilisierung die Anforderungen an ein Mindestmaß der IT-Sicherheit für die Zielgruppe benennt und eine Checkliste anbietet.

2.2 Muster-IT-Sicherheitskonzept mittlere und große kirchliche Einrichtungen

Mittlere und große Einrichtungen werden wie folgt definiert: diese Einrichtungen verfügen über eigenes geschultes IT-Personal oder Externe sowie eine professionelle IT-Infrastruktur mit eigenen Servern. Zudem existieren in der Regel bereits unterschiedlich ausgeprägte IT-Standards (z. B. Datensicherung, Kennwortregelungen, Protokollierung). Es gibt z. T. auch Dienstleistungen, die durch Outsourcing betrieben werden.

Darüber hinaus ist grundsätzlich immer nach dem Muster für mittlere und große kirchliche Einrichtungen vorzugehen, wenn eigenständig Daten mit hohem und sehr hohem Schutzbedarf verarbeitet werden.

Bei der Ausarbeitung dieses Musters war von vorn herein erkennbar, dass grundsätzlich die Vorgehensweise der BSI Standards 100-2 und 100-3 als Mindestmaß umzusetzen ist. Da dabei jedoch häufig eine Einstiegshürde vorhanden und nicht sofort das anzustrebende Ergebnis erkennbar ist, wurde in den Workshops ein Dokument als Muster-IT-Sicherheitskonzept mit jeweils erläuternden Beispielen und einer Kapitelstruktur des Vorgehens bei seiner Erstellung bereitgestellt.

2.3 „Bauplan“ Anwendung Muster-IT-Sicherheitskonzept mittlere und große kirchliche Einrichtungen

Der Bauplan ist ein Dokument, welches den Aufbau eines IT-Sicherheitskonzeptes grafisch darstellt.

2.4 Konzept zur Umsetzung von Schulung und Sensibilisierung

Um IT-Sicherheit erfolgreich umzusetzen sind Schulungen und Sensibilisierungen erforderlich. Nur auf diese Weise lässt sich langfristig eine Sicherheitskultur im Bereich der EKD, ihrer Gliedkirchen, gliedkirchlichen Zusammenschüsse, Diakonischen Werke und Einrichtungen etablieren. Dazu wurde ein Konzept erarbeitet, welches in Bezug auf die verschiedenen Zielgruppen, Empfehlungen zu Themen und Vorgehensweisen enthält und für die praktische Umsetzung auf allen Ebenen geeignet ist.

2.5 Präsentation mit einer Empfehlung zur Tool-Auswahl

Insbesondere bei der Umsetzung von IT-Sicherheitskonzepten in mittleren und großen kirchlichen Einrichtungen wird die Anwendung der Vorgehensweise nach den BSI Standards 100-2 und 100-3 oft hilfreich durch Werkzeuge unterstützt. Es wurde eine Gegenüberstellung der gängigen und geeigneten Tools mit den jeweiligen Leistungsmerkmalen erstellt.

2.6 Beispielhafte Schutzbedarfsfeststellung

Während der Workshops wurde für die Verfahren und Datenarten Meldewesen, Personalwesen, Finanzwesen und für Patientendaten der Diakonie eine Schutzbedarfsfeststellung beispielhaft durchgeführt.

Die Ergebnisse sind den Ergebnisdokumenten mit dem eindeutigen Vermerk „Muster“ hinzugefügt, da sie einen Überblick über die möglichen Ergebnisse einer Schutzbedarfsfeststellung illustrieren. Diese beispielhafte Schutzbedarfsfeststellung darf nicht ohne vorherige Überprüfung und Anpassung an die eigene Situation verwendet werden.

IMPRESSUM

Evangelische Kirche in Deutschland (EKD)

Herrenhäuser Straße 12, 30419 Hannover
Telefon: +49 511 2796 0
info@ekd.de
www.ekd.de

Verantwortlich: Arbeitsgruppe Muster-IT-Sicherheitskonzepte
Weitere Informationen: Koordinierungsstelle-IT@ekd.de
Download: www.ekd.de/EKD-Texte/muster_IT_sicherheitskonzepte

Juli 2015

Mitglieder der Arbeitsgruppe IT-Sicherheitskonzepte sind:

- Harald Aulenbacher, Kirchenamt der EKD
- Stefan Haas, Evangelische Landeskirche in Baden
- Lars Karrock, Evangelische Kirche in Hessen und Nassau
- Andrea Niemeyer, Kirchenamt der EKD
- Daniel Piasecki, Evangelisch-Lutherische Kirche in Norddeutschland
- Fabian Spier, Evangelisch-lutherische Landeskirche Hannovers
- Dr. Sascha Tönnies, Der Beauftragte für den Datenschutz der EKD
- Michael Werker, Diakonie Schleswig-Holstein
- Julian Wijnmaalen, Kirchenamt der EKD

Begleitende Beratung

HiSolutions AG
info@hisolutions.com
www.hisolutions.com
Bouchéstraße 12
12435 Berlin
Telefon: +49 30 533 289 0
Telefax: + 49 30 533 289 900
Theodor-Heuss-Ring 23
50668 Köln
Telefon: +49 221 771 09-550