VORSCHLÄGE FÜR EIN SCHULUNGS-KONZEPT IT-SICHERHEIT

Version 1.0

EVANGELISCHE KIRCHE IN DEUTSCHLAND

INHALTSVERZEICHNIS

1 ALLGEMEINES

1.1 Rahmenbedingungen / Ausgangslage

Die Evangelische Kirche in Deutschland EKD hat mit der Novellierung ihres Datenschutzgesetzes (DSG-EKD) sowie dem Erlass einer Ratsverordnung zur IT-Sicherheit sich, die Gliedkirchen, die gliedkirchlichen Zusammenschlüsse sowie die ihnen zugeordneten kirchlichen und diakonischen Werke und Einrichtungen zur Einhaltung der IT-Sicherheit und zur Erstellung, Umsetzung und Fortschreibung von IT-Sicherheitskonzepten verpflichtet.

1.2 Zielsetzung und Gegenstand

Um eine zielgerichtete und effiziente Erstellung und Umsetzung des IT-Sicherheitskonzeptes zu unterstützen, soll dieses Schulungskonzept Verantwortliche der wesentlichen Zielgruppen Wissen vermitteln und sie bezüglich IT-Sicherheit sensibilisieren.

1.3 Akzeptanzmanagement

Akzeptanzmanagement soll ermöglichen, dass das Thema IT-Sicherheit und die IT-Sicherheitskonzepte in den verschiedenen Einrichtungen verankert und gelebt werden. Ziel ist hierbei die Vermittlung der Sinnhaftigkeit von IT-Sicherheit sowie der Formulierung und des Einsatzes von IT-Sicherheitskonzepten.

Akzeptanzmanagement beantwortet die Frage, was würde die verschiedenen Mitarbeitergruppen dazu bewegen, Sicherheit einzuhalten. Der Erfahrung nach spielen zwei wichtige Faktoren die Hauptrolle:

- Der Bezug zur eigenen Arbeit (oder zum Privatleben) muss stets hergestellt werden: Bsp.: Handhabung von Passwörtern.
- Der Bezug zur eigenen Verantwortung muss stets hergestellt werden, z. B.: Was ist meine Rolle, meine Aufgabe? Daraus ergibt sich, welche Daten ich benutze: die Klassifizierung. Wer klassifiziert, der schützt!

2 ZIELGRUPPEN

Das Identifizieren und Schulen verschiedener Zielgruppen ist von enormer Bedeutung, damit eine Wissensvermittlung zielgerichtet und effizient durchgeführt werden kann.

Beim Workshop der Projektgruppe zur IT-Sicherheit im Mai 2014 wurden die folgenden zu adressierenden Zielgruppen identifiziert:

- Ehrenamtliche
- Angestellte (Verwaltung)
- Angestellte (Gemeinde/Basis)
- IT-Mitarbeiter
- Führungskräfte (Theologen, Juristen und sonstige Führungskräfte aus der Verwaltung)

2.1 Ehrenamtliche

Die Ehrenamtlichen sind eine sehr wichtige Zielgruppe und stellen zahlenmäßig die größte Gruppe aller Mitarbeitenden der evangelischen Kirche. Aufgrund der hohen Zahl von Ehrenamtlichen kann in der Regel die Wissensvermittlung nur in Bezug auf die durch den Ehrenamtlichen wahrgenommene Aufgabe durchgeführt werden.

2.2 Angestellte (Gemeinde/Basis)

Die Angestellten der Gemeinden haben mitunter sehr enge Berührungspunkte mit IT-Anwendungen und den damit verarbeiteten Daten. Eine kontinuierliche Wissensvermittlung unter Beachtung der dezentralen Standortgegebenheiten ist ratsam, damit das Wissen weiter vertieft und eine Sensibilisierung nachhaltig stattfinden kann.

2.3 Angestellte (Verwaltung)

Die Angestellten der Kirchenverwaltungen arbeiten täglich mit IT-Anwendungen und den damit verarbeiteten Daten. Eine kontinuierliche Wissensvermittlung vor Ort in der eigenen Verwaltung ist ratsam, damit das Wissen weiter vertieft und eine Sensibilisierung nachhaltig stattfinden kann.

2.4 IT-Mitarbeiter

IT-Mitarbeiter sorgen in der Regel für die Umsetzung des IT-Sicherheitskonzepts auf technischer und auch organisatorischer Ebene.

Damit IT-Mitarbeiter zielgerichtet und effektiv das IT-Sicherheitskonzept umsetzen können, sollte eine intensive Wissensvermittlung erfolgen.

2.5 Führungskräfte

Mit Führungskräften sind Theologen, Juristen und sonstiges Führungskräfte in der Regel aus der Verwaltung gemeint. Ein IT-Sicherheitskonzept ist nur dann erfolgreich, ein bestimmtes Sicherheitsniveau zu erreichen, wenn die Führungskräfte eindeutig die Notwendigkeit verstehen, hinter den Maßnahmen stehen, sie selbst vorleben sowie diese aktiv auch von ihren Mitarbeitern einfordern.

Gerade bei Führungskräften ist es wichtig, ein grundlegendes Verständnis für die oft sehr abstrakt und hochtechnisch erscheinenden Maßnahmen des IT-Sicherheitskonzeptes zu erreichen. Zudem sollte den Führungskräften deutlich gemacht werden, dass die Ziele der IT-Sicherheit wichtig für die Organisation sind.

3 METHODEN

In diesem Kapitel werden die Methoden der Wissensvermittlung skizziert, die in einem Schulungsprogramm zur Anwendung kommen. Im Folgenden werden die hier aufgezählten Methoden erläutert:

- Präsentation zum IT-Sicherheitsmanagement von externen Experten
- Kombinierter Vortrag zu Datensicherheit und IT-Sicherheit
- Schulung IT-Sicherheitskonzept inklusive Workshop
- E-Learning
- Handzettel zur IT-Sicherheit

3.1 Präsentation zum IT-Sicherheitsmanagement von externen Experten

Präsentationen haben im Allgemeinen den Vorteil, dass die Zielgruppen das Thema bzw. die Inhalte sehen und zusätzlich durch den Vortragenden hören. Diese Präsentation sollte inhaltlich alle wesentlichen Aspekte zur Informationssicherheit mit Beispielen beinhalten. Eine Präsentation von externen Experten wird an dieser Stelle empfohlen, damit durch dessen Expertise Gespräche mit den Zielgruppen über die Sicherheitsthemen gefördert wird. Des Weiteren wird ebenfalls durch Externe die Sicht auf IT-Sicherheit geschärft, was die interne IT weniger einem Rechtfertigungsdruck aussetzt. Eine Veranstaltung von mindestens einem halben Tag ist zu empfehlen.

Bei der Aufbereitung der Themen ist besonders darauf zu achten, einen nicht technischen aber sehr aggregierten Blick einzunehmen.

3.2 Kombinierter Vortrag zu Datensicherheit und IT-Sicherheit

Besonders Angestellte aus Gemeinden und der Verwaltung sollten in dieser Veranstaltung einen Einblick in die Datenschutzanforderungen in der EKD und auch in Maßnahmen der IT-Sicherheit bekommen. Für die Übermittlung des Wissens wird eine Powerpoint-Präsentation vorgeschlagen und für eine dezentrale Schulung sollte ein E-Learning-Tool (= E-Learning-Plattform, siehe 3.4) in Betracht gezogen werden. Für den kombinierten Vortrag ist mindestens ein halber Tag anzusetzen. Das E-Learning sollte quartalsweise erfolgen.

3.3 Schulung IT-Sicherheitskonzept

Das Knowhow, um ein Sicherheitskonzept nach dem Muster IT-Sicherheitskonzept zu erstellen, sollte den IT-Mitarbeitern, die für IT-Sicherheitsbelange zuständig sind, durch eine Schulung vermittelt werden. Dabei ist das theoretische Wissen durch einen Experten mithilfe von Präsentationen darzulegen und durch praktische Übungen zu ergänzen. Es wird empfohlen den Teilnehmerkreis von mindestens 8 bis maximal 15 Schulungsteilnehmern zu beschränken.

Aufbauempfehlung für eine Schulung zum IT-Sicherheitskonzept:

- 1. Tag: Theoretische Wissensvermittlung
- 2. Tag: Wiederholung und Vertiefung der Theorie anhand von Praxisbeispielen
- 3. Tag: Toolschulung (zur Durchführung des IT-Sicherheitskonzeptes) mit prakt. Übungen

3.4 E-Learning

Das Nutzen einer E-Learning Plattform ist eine moderne Art der nachhaltigen und günstigen Wissensvermittlung.

Im Bereich der IT-Sicherheit sind bisher leider nur wenige solcher Plattformen verfügbar. Eine günstige und ausgereifte Plattform ist das sogenannte „BITS (Behörden-IT-Sicherheitstraining“)[1]. Diese Web-Plattform (siehe Abbildung 1) bietet eine Auswahl an wichtigen Themen:

- E-Mail
- Viren
- Passworte
- Internet
- Vertrauliche Daten
- Mobile Geräte
- Am Arbeitsplatz

Es ist möglich diese Themen weiter zu entwickeln und somit auf spezifische Belange der evangelischen Kirche einzugehen.

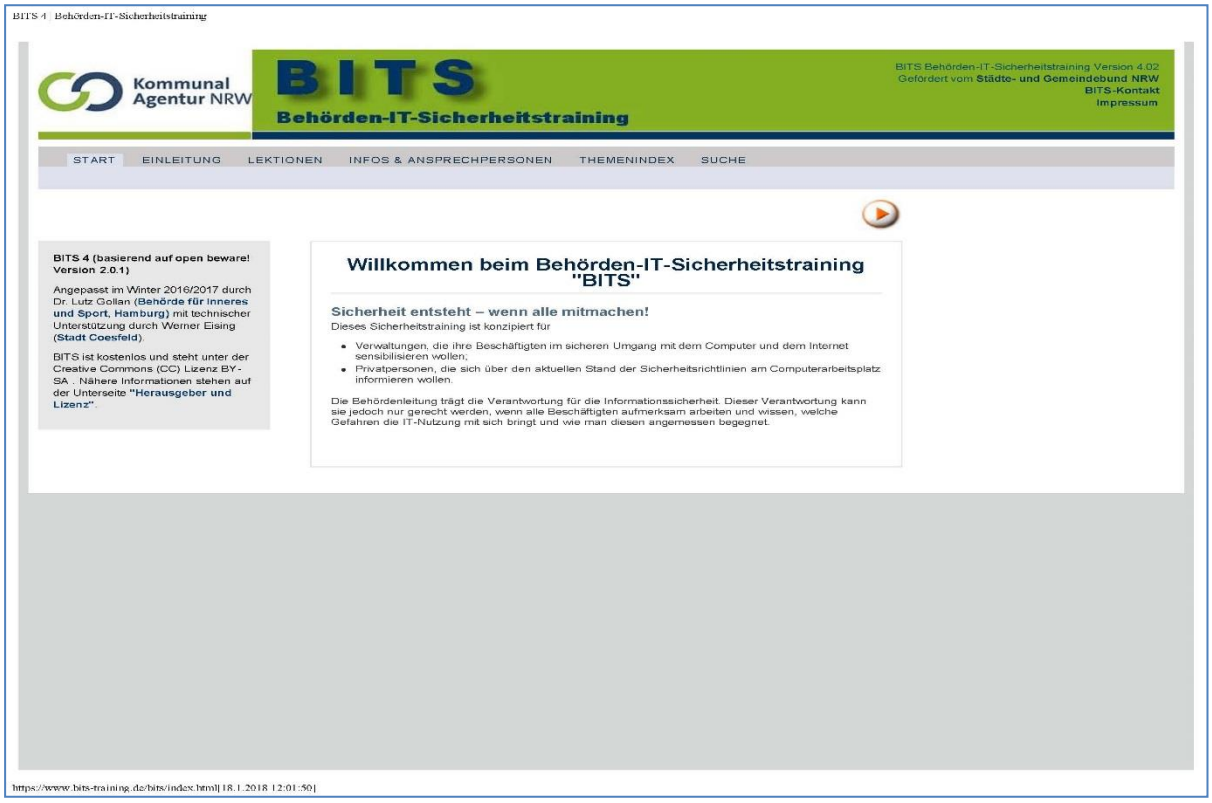


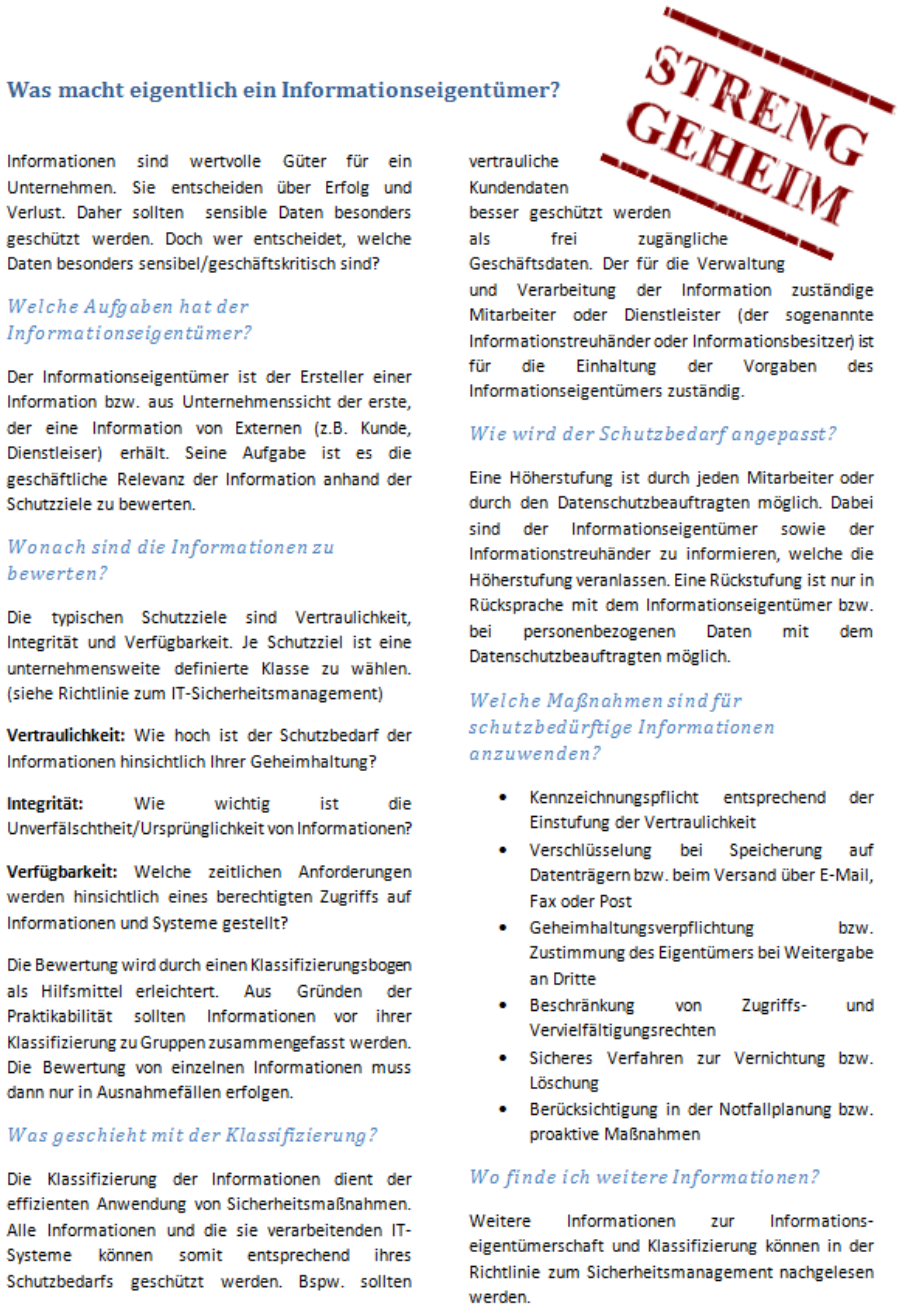
Abbildung 1: E-Learning Plattform "Behörden-IT-Sicherheitstraining BITS"

[1] Siehe https://www.bits-training.de/bits/index.html

3.5 Handzettel zur IT-Sicherheit

Zur weiteren Informationsvermittlung eignen sich Handzettel bzw. Informationsblätter. Auf diesen A-4 großen Seiten können bestimmte Themen aus dem großen Bereich der IT-Sicherheit vertieft, oder auch anwenderspezifisch und individuell auf die jeweilige Einrichtung abgestimmt, vermittelt werden. Eine Weitergabe des Wissens bzw. der Handzettel ist hier weniger aufwendig, da diese als E-Mail oder als ausgedrucktes Papier verteilt werden kann. Um die Zielgruppen nicht mit Sicherheitsinformationen zu überfordern, ist zu empfehlen, nicht mehr als zwei solcher Blätter im Jahr zu verteilen.

Die Abbildung 1 stellt ein Beispiel zum Thema Informationsklassifizierung dar.



Was macht eigentlich ein Informationseigentümer?

Informationen sind wertvolle Güter für ein Unternehmen. Sie entscheiden über Erfolg und Verlust. Daher sollten sensible Daten besonders geschützt werden. Doch wer entscheidet, welche Daten besonders sensibel/geschäftskritisch sind?

Welche Aufgaben hat der Informationseigentümer?

Der Informationseigentümer ist der Ersteller einer Information bzw. aus Unternehmenssicht der erste, der eine Information von Externen (z.B. Kunde, Dienstleiser) erhält. Seine Aufgabe ist es die geschäftliche Relevanz der Information anhand der Schutzziele zu bewerten.

Wonach sind die Informationen zu bewerten?

Die typischen Schutzziele sind Vertraulichkeit, Integrität und Verfügbarkeit. Je Schutzziel ist eine unternehmensweite definierte Klasse zu wählen. (siehe Richtlinie zum IT-Sicherheitsmanagement)

Vertraulichkeit: Wie hoch ist der Schutzbedarf der Informationen hinsichtlich Ihrer Geheimhaltung?

Integrität: Wie wichtig ist die Unverfälschtheit/Ursprünglichkeit von Informationen?

Verfügbarkeit: Welche zeitlichen Anforderungen werden hinsichtlich eines berechtigten Zugriffs auf Informationen und Systeme gestellt?

Die Bewertung wird durch einen Klassifizierungsbogen als Hilfsmittel erleichtert. Aus Gründen der Praktikabilität sollten Informationen vor ihrer Klassifizierung zu Gruppen zusammengefasst werden. Die Bewertung von einzelnen Informationen muss dann nur in Ausnahmefällen erfolgen.

Was geschieht mit der Klassifizierung?

Die Klassifizierung der Informationen dient der effizienten Anwendung von Sicherheitsmaßnahmen. Alle Informationen und die sie verarbeitenden IT-Systeme können somit entsprechend ihres Schutzbedarfs geschützt werden. Bspw. sollten vertrauliche Kundendaten besser geschützt werden als frei zugängliche Geschäftsdaten. Der für die Verwaltung und Verarbeitung der Information zuständige Mitarbeiter oder Dienstleister (der sogenannte Informationstreuhänder oder Informationsbesitzer) ist für die Einhaltung der Vorgaben des Informationseigentümers zuständig.

Wie wird der Schutzbedarf angepasst?

Eine Höherstufung ist durch jeden Mitarbeiter oder durch den Datenschutzbeauftragten möglich. Dabei sind der Informationseigentümer sowie der Informationstreuhänder zu informieren, welche die Höherstufung veranlassen. Eine Rückstufung ist nur in Rücksprache mit dem Informationseigentümer bzw. bei personenbezogenen Daten mit dem Datenschutzbeauftragten möglich.

Welche Maßnahmen sind für schutzbedürftige Informationen anzuwenden?

- Kennzeichnungspflicht entsprechend der Einstufung der Vertraulichkeit
- Verschlüsselung bei Speicherung auf Datenträgern bzw. beim Versand über E-Mail, Fax oder Post
- Geheimhaltungsverpflichtung bzw. Zustimmung des Eigentümers bei Weitergabe an Dritte
- Beschränkung von Zugriffs- und Vervielfältigungsrechten
- Sicheres Verfahren zur Vernichtung bzw. Löschung
- Berücksichtigung in der Notfallplanung bzw. proaktive Maßnahmen

Wo finde ich weitere Informationen?

Weitere Informationen zur Informations-eigentümerschaft und Klassifizierung können in der Richtlinie zum Sicherheitsmanagement nachgelesen werden.

Abbildung 2: Beispielhafter Handzettel zur Informationsklassifizierung

3.6 Weitere Sensibilisierungsmaßnahmen

Zur Unterstützung der oben genannten Methoden, sollten weitere Sensibilisierungsmaßnahmen eingeführt werden, damit die Aufmerksamkeit bei den Zielgruppen aufrechterhalten wird. Dazu eignen sich bspw.

- Newsletter per E-Mail,

- Flyer über die sichere Passwortgestaltung,
- Passwortkarten zur Hinterlegung von sicheren Passwörtern,
- Plakate mit speziellen Sicherheitsthemen,
- Notizzettel mit Sicherheitsempfehlungen,
- Sicherheitsrätsel mit Gewinnspiel.

Abbildung 3: Beispielhafte Passwortkarte zur einfachen Erstellung und Nutzung von Passwörtern mit entsprechender Güte

4 THEMEN

4.1 IT-Sicherheit (allgemein)

Die Inhalte zur IT-Sicherheit sind nach der jeweiligen Zielgruppe zu wählen. Damit sollten für Ehrenamtliche und Angestellte eher Themen zugeschnitten werden, welche die Anwendung der IT-Sicherheit betrifft. Dies sind u.a. Themen wie

- Informationen zur Anwendung der jeweiligen Richtlinien,
- Erstellen und Hinterlegen von Passwörtern,
- sichere IT-Nutzung.

4.2 IT-Sicherheitsmanagement

Die IT-Mitarbeitenden, welche bei der Umsetzung des Sicherheitskonzepts mitwirken sowie Verantwortung tragen, sollten neben den allgemeinen und o.g. Sicherheitsthemen in die Vorgehensweise nach BSI IT-Grundschutz geschult werden. Die folgenden Themen sind dabei zu berücksichtigen:

- Standards und Kataloge im IT-Grundschutz
- Aufbau und Struktur
- IT-Grundschutz-Vorgehensweise:
    - Definition Informationsverbund
    - IT-Strukturanalyse
        - Komplexitätsreduktion
        - Erhebung der IT-Systeme
        - Erhebung der Anwendungen
        - Erhebung der Netze
        - Erhebung der Standorte
        - Netzplanerhebung
    - Schutzbedarfsfeststellung
    - Modellierung
        - Schichtenprinzip
        - Bausteinaufbau und -struktur
    - Basissicherheitschecks
    - ergänzende Sicherheitsanalyse
    - Risikoanalyse

4.3 Verantwortung von Führungskräften

Für Führungskräfte gelten neben den allgemeinen Sicherheitsthemen als Anwender besonders Themen in Bezug auf deren Beitrag und Verantwortung.

Dabei sind die Themen so zu gestalten, dass die Führungskräfte an das Thema IT-Sicherheit herangeführt und darauf aufbauend auf deren Belange vertieft werden.

Dabei sollten folgende Inhalte thematisiert werden:

- IT-Sicherheit

  Was ist unter IT-Sicherheit zu verstehen?

  Aus welchen Gründen sollte IT-Sicherheit umgesetzt werden (Stellenwert der IT-Sicherheit)?

  Welche Motivationen / Hintergründe existieren IT-Sicherheit einzuhalten und stetig weiter zu entwickeln?

- Grundlagen zur Vorgehensweise nach BSI IT-Grundschutz
- Vorteile einer Zertifizierung nach BSI IT-Grundschutz
- Sicherheitsziele
- Beteiligung der Führungskräfte beim Managementprozess IT-Sicherheit
- Sicherheitsrisiken und deren Analyse
- Führungskräfte als Vorbildfunktion

4.4 Pflichten der Mitarbeitenden

Zu den Pflichten der Mitarbeiter gehört der verantwortungsvolle Umgang mit der IT. In den folgenden Themen sind alle Mitarbeitenden sinnvollerweise zu sensibilisieren:

- 10 goldenen Regeln zur IT-Sicherheit
- Richtlinien,
- Datenschutz,
- Sicherheitsvorfall,
- Soziale Netzwerke,
- Mobile Geräte,
- Social Engineering am Telefon.

Auch ein Hinweis auf das Organisationsverschulden bei mangelhafter Umsetzung der IT-Sicherheit durch die Mitarbeitenden sollte gegeben werden.

4.5 Herleitung von Risiken

Das Thema der Herleitung von Risiken für die kirchlichen Organisationen ist am besten durch die Vermittlung der Risikoanalyse-Grundlagen zu vermitteln. Hier sind die folgenden Aspekte zu adressieren:

- Bestimmung sowie Unterschiede zu Gefährdung und Risiko
- Ermitteln von Gefährdungen
- Gefährdungsbewertung – von der Gefährdung zum Risiko
- Risikobehandlung
- OPTIONAL: Risikoanalyse nach BSI Standard 100-3

4.6 Aufwand und Nutzen

Eine Abschätzung von Aufwänden für die Durchführung eines IT-Sicherheitskonzeptes ist nicht trivial und hängt immer von der Größe und dem Umfang des betrachteten Informationsverbundes sowie auch entscheidend vom Wissen der Verantwortlichen und Administratoren zur IT-Sicherheit ab.

Ein thematischer Aspekt einer Schulung zur Durchführung eines IT-Sicherheitskonzeptes sollte auch immer je nach Organisation eine ungefähre Einschätzung und Evaluierung möglicher Aufwände sowie eine Abwägung von Aufwand und Nutzen beinhalten.

5 SCHULUNGSPROGRAMM

Die folgende Tabelle 1 gibt eine Empfehlung zu einem möglichen Schulungsprogramm.

Tabelle 1: Schulungsprogramm

	Ehren-amtliche	**Angestellte (Gemeinden /Basis)**	**Angestellte (Verwaltung)**	**IT-Mitarbeitende**	**Führungs-kräfte**
Präsentation zum IT-Sicherheits-management				X	X
Kombinierter Vortrag zu Datensicher-heit und IT-Sicherheit		X	X		
Schulung IT-Sicherheits-konzept		X		X	
E-Learning	X	X	X		
Handzettel zur IT-Sicherheit	X	X	X	X	X
Weitere Sen-sibilisie-rungsmaß-nahmen	X	X	X	X	

VERZEICHNISSE

Abbildungsverzeichnis

Tabellenverzeichnis

KONTAKT

Evangelische Kirche in Deutschland

Koordinierungsstelle-IT@ekd.de

Herrenhäuser Straße 12

30419 Hannover

Telefon: +49 511 2796 0

Telefax: +49 511 2796 700

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