Muster-IT-Sicherheitskonzept für Beispiel-Kirchengemeinde

1. Einleitung

Alle kirchlichen Einrichtungen[1] sind für IT-Sicherheit verantwortlich. Informations- und Kommunikationstechnik (IT) ist in heutiger Zeit ein unverzichtbares Instrument zur Erfüllung von Aufgaben kirchlicher Stellen im Bereich der evangelischen Kirchen und ihrer Diakonie. IT-Sicherheit stellt einen Teil der Informationssicherheit dar. Diese umfasst die Sicherheit von IT-Systemen und der darin gespeicherten Daten durch Realisierung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung der Schutzziele der IT-Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit).

Die Vorgaben des Datenschutzes sind im EKD-Datenschutzgesetz (DSG-EKD) in der Novellierung aus dem Jahre 2013 formuliert. Aufgabe des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch die Verarbeitung und den Umgang seiner personenbezogenen Daten in dem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen ("informationelles Selbstbestimmungsrecht").

Alle Beschäftigten sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten bzw. darüber zu unterrichten.

Alle Mitarbeitenden und sonstige relevante Personen (extern Beschäftigte und Projektmitarbeiter) werden systematisch und zielgruppengerecht zu Datenschutzfragen sensibilisiert und zum Umgang mit personenbezogenen Daten geschult.

Es sind technisch-organisatorische Verfahren gemäß § 9 Absatz 1 DSG-EKD zu entwickeln, um die Durchsetzung der Rechte der Betroffenen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht in bestehende Bestandsverzeichnisse sicherzustellen.

Somit müssen auch die kleinen kirchlichen Einrichtungen Maßnahmen zur Informationssicherheit umsetzen. Mit dieser Richtlinie und der im Anhang enthaltenen Checkliste zur Informationssicherheit soll diesen Organisationen ein Werkzeug an die Hand gegeben werden. Dieses Dokument muss regelmäßig fortgeschrieben und mit der/dem zuständigen IT-Sicherheitsbeauftragte/-en abgestimmt werden. Es bietet sich an, die Regelungen und die Checkliste quartalsweise oder in kürzeren Intervallen, mindestens aber einmal im Jahr zu überprüfen und ggf. anzupassen. Hierbei muss man sich der Tatsache bewusst sein, dass IT-Sicherheit kein statischer Zustand ist, sondern sich in einem stetigen Prozess fortentwickelt.

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.

Mittlere und große Einrichtungen hingegen verfügen über eigenes geschultes IT-Personal oder externe Mitarbeitende sowie über 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. Dienstleistungen, die durch Outsourcing betrieben werden.

Informationssicherheit sorgt dafür, dass die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit gewahrt werden. Vertraulichkeit schützen bedeutet, die IT-Systeme und Anwendungen so zu sichern, dass nur autorisierte Personen auf die verarbeiteten Daten Zugriff haben. Integrität schützt die Daten vor Mani-

[1] siehe § 1 Absatz 2 DSG-EKD

pulationen. Verfügbarkeit hingegen sorgt dafür, dass Daten im gewünschten Zeitraum zur Verfügung stehen und darauf zugegriffen werden kann.

2. Checkliste für kleine Organisationen

Die folgende Checkliste dient als Umsetzungshilfe für die Prüfung und Dokumentation des Umsetzungszustandes der Sicherheitsmaßnahmen für kleine Einrichtungen. Die Checkliste kann ebenso als Nachweis der Bemühungen zur Umsetzung der IT-Sicherheit verwendet werden.

Nr.	Frage	Referenz	Umgesetzt
1.	Werden neue Mitarbeitende bei der Einstellung auf bestehende Regelungen und Handlungsanweisungen zur Informationssicherheit hingewiesen?	Kap. 3	□
2.	Sind die wichtigen Schlüsselpositionen durch einen Vertreter besetzt?	Kap. 3	□
3.	Haben alle Mitarbeitenden eine Verpflichtung zur Wahrung des Datengeheimnisses unterschrieben?	Kap. 3	□
4.	Werden Backup-Datenträger in einem gesonderten Raum aufbewahrt?	Kap. 4	□
5.	Sind auf allen Clients Virenschutzprogramme installiert?	Kap. 6	□
6.	Werden Betriebssysteme und Anwendungen regelmäßig aktualisiert?	Kap. 6	□
7.	Gibt es eine Checkliste für Mitarbeitende zur Beendigung des Arbeitsverhältnisses?	Kap. 6	□
8.	Gibt es eine Benutzer- und Rechteverwaltung für IT-Systeme und Anwendungen?	Kap. 6	□
9.	Gibt es Passwortregelungen für IT-Systeme und Anwendungen und werden diese umgesetzt?	Kap. 6	□
10.	Werden alle Mitarbeitenden über die Regelungen zur Nutzung von Standardsoftware informiert?	Kap. 6	□
11.	Wird ausschließlich Software aus vertrauenswürdigen Quellen installiert?	Kap. 6	□
12.	Gibt es regelmäßige Kontrollen bezüglich der installierten Software?	Kap. 6	□
13.	Sind auf Clients und Servern automatische Updates aktiviert?	Kap. 6	□
14.	Gibt es spezielle Handlungsanweisungen und Tools zum Löschen und Vernichten von Daten?	Kap. 6	□
15.	Sind Türen und Fenster in der Regel verschlossen, wenn die Mitarbeitenden nicht am Platz sind?	Kap. 7	□
16.	Sind in den Büros verschließbare Schreibtische oder Schränke vorhanden?	Kap. 7	□

17.	Gibt es in Büros mit Publikumsverkehr Diebstahlsicherungen für IT-Systeme?	Kap. 7	□
18.	Sind am mobilen Arbeitsplatz verschließbare Schreibtische oder Schränke vorhanden?	Kap. 8	□
19.	Gibt es Regelungen welche dienstlichen Unterlagen am häuslichen Arbeitsplatz bearbeitet und zwischen der Institution und dem häuslichen Arbeitsplatz hin und her transportiert werden dürfen?	Kap. 8	□
20.	Ist auf allen Clients die Bildschirmsperre aktiviert?	Kap. 9	□
21.	Ist der Zugriff von mobilen Laptops auf das LAN per VPN abgesichert?	Kap. 9	□
22.	Ist die Verschlüsselung von E-Mail-Kommunikation zwischen Client und Server aktiviert?	Kap. 9	□
23.	Ist bei allen Mobiltelefonen/Smartphones die Eingabe der Geräte-PIN aktiviert?	Kap. 10	□
24.	Werden alle vertraulichen Daten nur verschlüsselt auf Mobiltelefonen/Smartphones oder Speicherkarten gespeichert?	Kap. 10	□
25.	Wird bei WLAN das Verschlüsselungsverfahren WPA2 eingesetzt?	Kap. 11	□
26.	Werden die Schlüssel für den WLAN-Zugriff regelmäßig gewechselt?	Kap. 11	□

3. Sensibilisierung der Mitarbeitenden

Besonders wichtig ist die Sensibilisierung aller relevanten Mitarbeitenden. Nur mit informierten und achtsamen Mitarbeitenden können Sicherheitsmaßnahmen wirksam umgesetzt und eventuelle Sicherheitsvorfälle rechtzeitig erkannt werden.

Sobald die Ursache eines Sicherheitsvorfalls identifiziert wurde, müssen Maßnahmen zu dessen Behebung ergriffen werden. Häufig ist es notwendig, die betroffenen IT-Systeme oder Standorte zu isolieren, um die Auswirkung des Sicherheitsvorfalls einzudämmen. Die Behebung von Sicherheitsvorfällen muss ausführlich dokumentiert werden.

Ein Beispiel für eine Sensibilisierung der Mitarbeitenden „Dienstanweisung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz“ befindet sich im Anhang C2 BFDI Musterformular.

4. Datensicherungskonzept

Computersysteme und Datenträger (z. B. Festplatten, Speicherkarten) können ausfallen oder manipuliert werden. Durch Verlust oder Veränderungen von gespeicherten Daten können mitunter gravierende Schäden verursacht werden. Durch regelmäßige Datensicherungen werden Schäden durch Ausfälle von Datenträgern, Schadsoftware oder Manipulationen an Datenbeständen nicht verhindert, deren Auswirkungen können aber minimiert werden.

Die zu sichernden Daten und Anwendungen (hauptsächlich dezentral) müssen aufgelistet und jeweils einem Verantwortlichen zugordnet werden.

Backup-Datenträger müssen einerseits im Bedarfsfall schnell verfügbar sein, andererseits sollten sie räumlich getrennt von den gesicherten IT-Systemen aufbewahrt werden. Somit sind sie auch bei Notlagen, wie z. B. Brand oder Hochwasser verfügbar.

Hinweis: Das zusätzliche Speichern auf einem vorzugsweise verschlüsselten USB-Stick könnte eine Datensicherung darstellen.

5. Schutz vor Schadprogrammen

Wenn IT-Systeme mit Schadsoftware (Viren, Würmer, Trojanische Pferde usw.) befallen werden, kann dies die Verfügbarkeit, Integrität und Vertraulichkeit der Systeme und der darauf gespeicherten Daten gefährden.

Es muss auf jedem IT-System (z. B. PC, Laptop) ein Viren-Schutzprogramm installiert werden. Automatische Updates müssen aktiviert sein. Dabei muss sichergestellt werden, dass auch die mobilen Endgeräte ausreichend geschützt sind.

Infizierte IT-Systeme müssen unverzüglich von allen Datennetzen getrennt und dürfen bis zur vollständigen Bereinigung nicht mehr produktiv genutzt werden.

Auf allen IT-Systemen müssen für die Betriebssysteme sowie für alle installierten Treiber und Programme zeitnah die jeweils hierfür veröffentlichten sicherheitsrelevanten Updates und Patches eingespielt werden. Dies gilt besonders für Programme, mit denen auf Fremdnetze zugegriffen wird (z. B. Webbrowser).

6. Regelungen für Hard- und Software

Für den sicheren Einsatz von IT-Systemen und IT-Anwendungen ist es erforderlich, dass Abläufe und Vorgänge, die diese IT-Systeme berühren, so gestaltet werden, dass das angestrebte Niveau der Informationssicherheit erreicht bzw. beibehalten wird.

Alle Mitarbeitenden müssen darüber informiert werden, dass nur explizit von der Einrichtung freigegebene und korrekt lizensierte Standardsoftware eingesetzt werden darf.

Es darf nur solche Software eingesetzt werden, für die noch regelmäßig Sicherheitsupdates und -patches ausgeliefert werden.

Durch eine geeignete Benutzerkonten- und Rechteverwaltung wird sichergestellt, dass nur diejenigen Personen Zugriff auf IT-Systeme, Applikationen und Informationen haben, die aufgrund ihrer Aufgaben dazu berechtigt sind.

Bei der normalen Nutzung der Clients darf nicht mit administrativen Rechten (Admin-Benutzer) gearbeitet werden. Dies ist nur zu administrativen Tätigkeiten zulässig, die unbedingt von normalen Aufgaben getrennt durchzuführen sind.

Um sicherzustellen, dass nur Befugte auf Systeme und Informationen zugreifen können, ist es wichtig, dass sich die Mitarbeitenden vor der Nutzung per Passwort authentisieren müssen. Die Benutzer müssen über die dafür notwendigen Regelungen und deren Anwendung sowie deren Hintergründe explizit informiert werden.

Das Passwort bei IT-Systemen muss aus mindestens 8 Zeichen bestehen. Es muss sich aus Klein- und Großbuchstaben, sowie aus Zahlen oder Sonderzeichen zusammensetzen.

Bei der Beendigung von Arbeitsverhältnissen ist die geordnete Über- und Rückgabe der Geräte und Daten sicherzustellen.

Das sichere Löschen und Vernichten von Daten auf Datenträgern (z.B. Server, Clients, Netzkomponenten, Smartphones) muss vor der Aussonderung oder vor einer Weitergabe der Datenträger und Geräte vorgenommen werden.

7. Büroraum / Lokaler Arbeitsplatz

Der Büroraum ist ein Raum, in dem sich eine oder mehrere Personen aufhalten, um dort der Erledigung ihrer Aufgaben nachzugehen. Diese Aufgaben können (auch IT-unterstützt) aus den verschiedensten Tätigkeiten bestehen: Erstellung von Schriftstücken, Bearbeitung von Karteien und Listen, Durchführung von Besprechungen und Telefonaten, Lesen von Akten und sonstigen Unterlagen.

Fenster und Türen sind zu verschließen, wenn ein Raum nicht besetzt ist. Büroräume müssen so ausgestattet sein, dass schutzbedürftige Datenträger und Dokumente weggeschlossen werden können. Dazu müssen beispielsweise verschließbare Schreibtische, Rollcontainer oder Schränke vorhanden sein.

Alle Mitarbeitenden müssen darauf hingewiesen werden, dass auch in Büroräumen die vorhandenen IT-Geräte, Zubehör, Software oder Daten ausreichend gegen Diebstahl, Zerstörung und Veränderungen geschützt werden.

In Büros mit Publikumsverkehr sind Diebstahlsicherungen zum Schutz von IT-Systemen (z. B. Laptops) einzusetzen, da andernfalls die Gefahr besteht, dass solche Geräte in einem unbewachten Augenblick abhandenkommen.

8. Mobiler Arbeitsplatz

Ein mobiler Arbeitsplatz kann auch z. B. von Telearbeitern, freien Mitarbeitern oder Selbstständigen sowie von Ehrenamtlichen genutzt werden. Bei einem mobilen Arbeitsplatz kann die infrastrukturelle Sicherheit nicht so vorausgesetzt werden, wie sie in einer Büroumgebung innerhalb der Räumlichkeiten einer Institution anzutreffen ist.

Dienstliche Aufgaben werden häufig auch an wechselnden Arbeitsplätzen und in unterschiedlichen Umgebungen durchgeführt. Die dabei verarbeitenden Informationen müssen angemessen geschützt werden (z. B. durch Sperren des Bildschirms oder Anbringen eines Sichtschutzes).

Die Leistungsfähigkeit von mobilen IT-Systemen wie beispielsweise Laptops, Handys und PDAs wächst ständig und lässt es zu, große Mengen geschäftsrelevanter Informationen außerhalb der Räume der jeweiligen Institution zu bearbeiten. Dabei ist zu beachten, dass meist die infrastrukturelle Sicherheit nicht der einer Büroumgebung entspricht.

An mobilen Arbeitsplätzen sollten weder dienstliche Unterlagen noch mobile IT-Systeme unbeaufsichtigt bleiben. Sie sollten zumindest gegen einfache Wegnahme gesichert, z. B. mit einer Diebstahlsicherung versehen oder in Schränke geschlossen werden.

Beim Einsatz mobiler Geräte sind die Festplatten der Rechner grundsätzlich immer zu verschlüsseln.

9. Arbeitsplatz-Rechner

Als Arbeitsplatz-Rechner wird ein IT-System mit einem beliebigen Betriebssystem bezeichnet, das die Trennung von Benutzern zulässt.

Eine Bildschirmsperre muss eingerichtet werden, die sich sowohl manuell vom Benutzer aktivieren lässt, als sich auch nach einem vorgegebenen Inaktivitäts-Zeitraum automatisch aktiviert.

Alle Mitarbeitenden sind dazu zu verpflichten, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden.

E-Mails müssen verschlüsselt von und zu Mail-Servern übertragen werden (z. B. mittels SSL/TLS). Die entsprechenden Einstellungen bei E-Mailprogrammen (SSL/TLS) sind standardmäßig vorzunehmen.

Ein Laptop oder Notebook ist ein IT-System mit einer transportfreundlichen, kompakten Bauform, welches aufgrund dieser mobil genutzt werden kann. Ein Laptop ist ein vollwertiger Arbeitsplatz-Rechner und kann über Akkus zeitweise unabhängig von externer Stromversorgung betrieben werden.

Bei diesen Geräten sind die Festplatten grundsätzlich zu verschlüsseln.

Zugriffe von einem Laptop von außerhalb auf das interne Netz müssen abgesichert erfolgen (über SSL/TLS oder VPN verschlüsselt).

10. Mobiltelefon / Smartphone

Mobiltelefone bzw. Smartphones sind inzwischen alltäglicher Bestandteil der kirchlichen Kommunikationsinfrastruktur geworden. Neben herkömmlichen Telefongesprächen bieten die Geräte meist noch eine Vielzahl an zusätzlichen Funktionen wie das Verschicken von SMS, MMS, E-Mails, die Nutzung des Internets über WLAN oder Mobilfunk. Zudem existieren auch Apps, wie z. B. Whatsapp oder Threema, die Funktionalitäten zur Datenübertragung ermöglichen.

Verlorene Geräte müssen über den Mobilfunkanbieter umgehend gesperrt werden.

Es muss sichergestellt werden, dass die Sicherheitsmechanismen von Mobiltelefonen (z. B. Eingabe einer PIN oder eines Passworts, Fingerabdruck, etc.) genutzt werden.

Bei der Verwendung von Mobiltelefonen muss entschieden werden, ob und wie zusätzliche Dienste wie MMS, Bluetooth oder WLAN genutzt werden dürfen. Nicht benötigte Dienste sollten deaktiviert werden.

Vertrauliche Daten, wie personenbezogene Daten oder Zugangsdaten zum Netz der Institution, sind prinzipiell nicht auf den Geräten zu speichern. Eine unumgängliche Speicherung auf dem Gerät (inklusive Speicherkarte) muss ausschließlich in verschlüsselter Form erfolgen. Das Senden von vertraulichen Daten ist nur über gesicherte, von der kirchlichen Organisation bereitgestellte Transportwege erlaubt. Nicht dazu gehören z. B. Skype, Whatsapp oder private E-Mail.

11. Netzwerke

Wireless LANs (WLANs) bieten die Möglichkeit, mit geringem Aufwand drahtlose lokale Netze aufzubauen oder bestehende drahtgebundene Netze zu erweitern. WLANs können aufgrund der einfachen Installation nicht nur dauerhaft, sondern auch für temporär zu installierende Netze, wie z. B. für Veranstaltungen, verwendet werden.

Die Kommunikation im WLAN sowie im Power-LAN muss verschlüsselt werden. Für WLAN ist WPA2 zu verwenden. Für Power-LAN ist mindestens eine Verschlüsselung mit AES-128 zu verwenden.

Es wird empfohlen die kryptographischen Schlüssel für den Zugriff auf ein WLAN zufällig zu wählen und diese regelmäßig zu wechseln. Voreingestellte Standardpasswörter sind vor Inbetriebnahme unbedingt zu wechseln.

Bei der Aussonderung von WLAN-Komponenten müssen die Authentifizierungsinformationen für den Zugang zum WLAN und andere erreichbare Ressourcen, die in der Sicherheitsinfrastruktur und anderen Systemen gespeichert sind, entfernt bzw. als ungültig deklariert werden. Hierzu ist die Komponente auf die Werkseinstellung zurückzusetzen.

12. Mobile Datenträger

Mobile Datenträger werden für eine Vielzahl von Zwecken eingesetzt, beispielsweise für den Datentransport, die Speicherung von Daten oder die mobile Datennutzung. Es gibt eine Vielzahl verschiedener Varianten von mobilen Datenträgern. Hierzu gehören unter anderem Disketten, externe Festplatten, CD-ROMs, DVDs, Magnetbänder und USB-Sticks.

Die Mitarbeitenden müssen über die Risiken in Hinblick auf mobile Datenträger und über die erforderlichen Sicherheitsmaßnahmen informiert werden.

Bei mobilen Datenträgern besteht ein hohes Verlust- und Diebstahlsrisiko. Damit die Daten nicht in falsche Hände geraten, sind die Dateien oder besser die gesamten mobilen Datenträger zu verschlüsseln. Insbesondere vertrauliche Dateien auf mobilen Datenträgern müssen zwingend verschlüsselt werden. Dazu bietet sich z. B. die freie Software 7zip mit AES-256 Bit Verschlüsselung an.

Hinweis: Um den Aufwand durch eine zusätzliche Software zu minimieren, sollte bevorzugt auf Lösungen zur Hardwareverschlüsselung zurückgegriffen werden (verschlüsselte USB-Sticks oder Festplatten).

13. Internetnutzung

Das Internet als wichtiges Informations- und Kommunikationsmedium ist aus dem Arbeitsalltag nicht mehr wegzudenken. In den meisten Organisationen ist die Nutzung von E-Mail, Informationsangeboten, Internet-Dienstleistungen, Online-Banking und Online-Shopping selbstverständlich. Gleichzeitig muss verhindert werden, dass durch die Anbindung der eigenen Geräte an das Internet für die Organisation nicht akzeptable Risiken entstehen.

Alle Mitarbeitenden sollten über das Potential, aber auch die Risiken der Internet-Nutzung informiert sein. Sie müssen wissen, welche Rahmenbedingungen bei der Nutzung von Internet-Diensten zu beachten sind. Dazu gehört insbesondere, dass sie die Regeln kennen, um Dienste sicher zu nutzen und sich korrekt im Internet zu verhalten, beispielsweise in (Web-)Blogs oder sozialen Netzwerken (z. B. Facebook, Twitter).

Bei vielen Internet-Diensten müssen sich die Benutzer mittels Benutzernamen und Passwort authentisieren. Dabei sind die allgemeinen Regeln zur sicheren Verwendung von Passwörtern (siehe Hard- und Software) einzuhalten. Wichtig ist insbesondere, dass die Passwörter nicht leicht zu erraten sind. Es sind für verschiedene Internet-Dienste verschiedene Passwörter zu verwenden. Vor allem sind dafür keine Passwörter zu nutzen, die für IT-Systeme oder IT-Anwendungen innerhalb der kirchlichen und diakonischen Einrichtungen verwendet werden.

Glossar

Begriff	Erläuterung
WPA2	Wi-Fi Protected Access 2 (WPA2) ist die Implementierung eines Sicherheitsstandards für Funknetzwerke.
AES-128	AES steht für Advanced Encryption Standard. Dies ist ein Verschlüsselungsstandard mit einer Schlüssellänge von 128 Bit.
TLS/SSL	Transport Layer Security (TLS) ist ein Protokoll zur Verschlüsselung von Datenübertragungen im Internet - weitläufiger bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (SSL).
VPN	Virtual Private Network (VPN) ist ein privates (in sich geschlossenes) Rechnernetz, das auf einer öffentlichen Netzwerk-Infrastruktur aufgebaut ist.
Patch	Ein Patch ist ein in der Regel kleineres Softwareupdate bzw. eine kleinere Softwarekorrektur.

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