Leitfaden zur Umsetzung der „IT-Sicherheitsverordnung“ für kirchliche Stellen

Vorbemerkung

Seit Mitte 2015 gilt die Verordnung der EKD zur Sicherheit in der Informationstechnik, kurz: „IT-Sicherheitsverordnung“.

Die Umsetzung der IT-Sicherheitsverordnung ist für jede kirchliche Stelle verpflichtend.

Die entsprechenden Dokumente zur IT-Sicherheitsverordnung können Sie über den folgenden link abrufen: https://kirchencloud.kigst.de/index.php/s/hXJYOUzcTgjNAtt

Was genau eine „kirchliche Stelle“ ist, ergibt sich aus § 1 Absatz 2 der IT-Sicherheitsverordnung. Hiernach gilt die IT-Sicherheitsverordnung für die EKD, ihre Gliedkirchen und gliedkirchlichen Zusammenschlüsse sowie die ihnen zugeordneten kirchlichen und diakonischen Werke und Einrichtungen ohne Rücksicht auf ihre Rechtsform und für rechtsfähige evangelische Stiftungen des bürgerlichen Rechts. Dementsprechend sind auch umfasst die Kirchenkreise und Kirchenkreisverbände, die Kirchengemeinden und Kirchengemeindeverbände und – ohne Rücksicht auf deren Rechtsform – deren rechtlich selbstständige Dienste und Werke.

Die Kernpunkte der IT-Sicherheitsverordnung sind:

- Jede kirchliche Stelle muss ein IT-Sicherheitskonzept erstellen.
- Es stehen Muster-IT-Sicherheitskonzepte zur Verfügung.
- Private IT-Geräte dürfen nur unter bestimmten Voraussetzungen verwendet werden.
- Es müssen Schulungs- und Fortbildungsmöglichkeiten für die Mitarbeitenden angeboten werden.
- Die IT-Sicherheitsverordnung gibt vor, dass die Umsetzung in Grundzügen bis zum 31.12.2015 und vollständig bis zum 31.12.2017 erfolgen muss.
- Die Verantwortung liegt beim Leitungsorgan der kirchlichen Stelle.
- Es können IT-Sicherheitsbeauftragte benannt werden, die auch mehrere kirchliche Stellen umfassen können.

Bei Nichtbeachtung oder Vernachlässigung der IT-Sicherheit besteht die Gefahr massiver Beeinträchtigung der betroffenen Personen sowie das Risiko von Reputations- oder wirtschaftlichen Verlusten für die jeweilige kirchliche Stelle, aber auch darüber hinaus.

Die Zuständigkeit hierfür geht über die jeweilige IT-Fachabteilung hinaus und bezieht alle handelnden Personen, Akteure und Dienststellen im Rahmen ihrer Tätigkeit mit ein. Jede Person kann und muss durch ihr Verhalten dazu beitragen.

IT-Sicherheit ist eine Aufgabe von hoher Priorität, für die das jeweilige Leitungsorgan der kirchlichen Stelle Verantwortung tragen muss und für Mitarbeitende eine obliegende Verpflichtung sein kann.

Mit diesem Leitfaden möchten wir Ihnen eine Hilfestellung geben, wie Sie ein IT-Sicherheitskonzept erstellen und zu welchen Zeitpunkten welche Maßnahmen umgesetzt sein müssen.

Was bedeutet IT-Sicherheit?

IT-Sicherheit ist ergänzender Teil zum Datenschutz. Der Datenschutz soll insbesondere dafür sorgen, dass die in den Kirchen vorhandenen sensiblen Daten und Aufzeichnungen (z.B. Mitgliederdaten, Personaldaten, Inhalte aus Seelsorgegesprächen) nicht in unbefugte Hände geraten.

IT-Sicherheit umfasst darüber hinaus die Sicherheit von IT-Systemen und der darin gespeicherten Daten durch Realisierung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen.

IT ist dabei so auszuwählen, zu nutzen und zu administrieren, dass für die damit verarbeiteten Daten zu jeder Zeit das angemessene Maß an **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** sichergestellt ist.

Bezüglich der Vertraulichkeit muss festgelegt werden, wer auf welche Daten zugreifen darf (Rechte- und Rollenkonzept für das jeweilige IT-System), eine unbefugte Preisgabe der Daten muss möglichst ausgeschlossen werden.

Hinsichtlich der Integrität muss eine unbefugte oder unkontrollierte Veränderung der Daten, der Software und Hardware möglichst ausgeschlossen sein.

Bezüglich der Verfügbarkeit muss sichergestellt werden, dass Daten dann zur Verfügung stehen, wenn sie zur Aufgabenerfüllung gebraucht werden. Gegebenenfalls eintretende Stillstandzeiten müssen in Ausnahmefällen toleriert werden können.

In den Bereichen, in denen hochsensible schutzbedürftige Daten erhoben, verarbeitet oder genutzt werden, insbesondere im Melde-, Kirchenbuch-, Personalwesen, Haushalts-, Kassen- und Rechnungswesen, sowie bei der Verwaltung von Klientendaten sind an die drei Schutzziele (Vertraulichkeit, Integrität und Verfügbarkeit) in der Regel hohe Anforderungen zu stellen.

Sicherheitsprüfungen vor Ort sollen umfassend durchgeführt werden und nicht nur einzelne IT-Komponenten betrachten. Dies erfordert ein auf die Gegebenheiten der jeweiligen kirchlichen Stelle abgestimmtes Gesamt-IT-Sicherheitskonzept.

Das Erstellung und Umsetzung des IT-Sicherheitskonzepts ist ein laufender und kontinuierlicher Prozess und besteht grundsätzlich aus den folgenden vier Schritten:

1. Dokumentation des Status Quo
2. Festlegung und Dokumentation der erforderlichen Maßnahmen zur Verbesserung der IT-Sicherheit
3. Umsetzung der definierten Maßnahmen
4. Verifikation der umgesetzten Maßnahmen

In einem ersten Schritt erfolgt die Bestandsaufnahme anhand einer „Checkliste“. (siehe Folgeseite)

Diese Checkliste umfasst 27 Fragen, die von dem Leitungsorgan der Kirchengemeinde (oder dem benannten IT-Sicherheitsbeauftragten) mit dem Status erfüllt bzw. nicht-erfüllt versehen werden muss.

Diese ausgefüllte Checkliste dient zum einen dem Nachweis der Bemühungen zur Umsetzung der IT-Sicherheitsverordnung und sollte daher bis zum 31.12.2015 erstellt werden.

Zum anderen ist sie die Basis für die Ermittlung der umzusetzenden Maßnahmen zur Erfüllung der IT-Sicherheitsverordnung, die zum 31.12.2017 abgeschlossen sein muss.

Checkliste für kirchliche Stellen

Die folgende Checkliste dient als Umsetzungshilfe für die Prüfung und Dokumentation des Umsetzungsstandes der Sicherheitsmaßnahmen in der kirchlichen Stelle und kann als Nachweis der Bemühungen zur Umsetzung der IT-Sicherheitsverordnung verwendet werden.

Bitte beachten Sie insbesondere die ergänzenden Hinweise!

Nr.	Verpflichtende Maßnahme	ergänzende Hinweise	erfüllt	nicht erfüllt
1.	Haupt- und ehrenamtliche Mitarbeitende sind auf bestehende Regelungen und Handlungsanweisungen zur Informationssicherheit (soweit vorhanden) hinzuweisen.	Kapitel 1	☐	☐
2.	Haupt- und ehrenamtliche Mitarbeitende müssen eine Verpflichtung zur Wahrung des Datengeheimnisses unterschreiben.	Kapitel 1	☐	☐
3.	Haupt- und ehrenamtliche Mitarbeitende sind darauf hinzuweisen, dass nur dienstliche und lizensierte Software anzuwenden ist, diese muss von dafür befugten Personen installiert werden.	Kapitel 1	☐	☐
4.	Es sind regelmäßige Kontrollen bezüglich der installierten Software durchzuführen.	Kapitel 1	☐	☐
5.	Für Personen, die wichtige, bspw. administrative IT-Aufgaben wahrnehmen, ist eine Vertretungsregelung festzulegen.	Kapitel 1	☐	☐
6.	Nur Personen, die administrative IT-Aufgaben haben, dürfen administrative Rechte für Soft- und Hardware besitzen.	Kapitel 1	☐	☐
7.	Für hauptamtliche Mitarbeitende ist eine Checkliste für die Beendigung des Arbeitsverhältnisses zu erstellen, die eine geordnete Über- und Rückgabe der Geräte und Daten sicherstellt. Dies gilt für ehrenamtliche Mitarbeitende entsprechend.	Kapitel 1	☐	☐
8.	Es sind regelmäßig Datensicherungen durchzuführen.	Kapitel 2	☐	☐
9.	Die zu sichernden Daten und Anwendungen sind aufzulisten und einem Verantwortlichen zuzuordnen.	Kapitel 2	☐	☐
10.	Datenträger mit Datensicherungen sind räumlich getrennt von den IT-Systemen aufzubewahren, so dass sie z.B. bei Brand oder Hochwasser verfügbar sind.	Kapitel 2	☐	☐

11.	Auf allen PCs, Notebooks, Tablets, usw. sind Virenschutzprogramme zu installieren und automatische Updates für Virenschutzprogramme sind zu aktivieren.	Kapitel 3	☐	☐
12.	Betriebssysteme und Anwendungen sind zeitnah mit den hierfür veröffentlichten sicherheitsrelevanten Updates zu aktualisieren.	Kapitel 3	☐	☐
13.	Für IT-Systeme und Anwendungen ist eine Benutzer- und Rechteverwaltung zu verwenden.	Kapitel 4	☐	☐
14.	Alle Personen müssen sich vor der Nutzung mit einem Passwort authentisieren.	Kapitel 4	☐	☐
15.	Für IT-Systeme und Anwendungen sind Passwortregelungen anzuwenden, die aus mindestens 8 Zeichen bestehen und sich aus Klein- und Großbuchstaben, sowie Zahlen oder Sonderzeichen zusammensetzen.	Kapitel 4	☐	☐
16.	Vor der Aussonderung oder Weitergabe von Geräten ist eine sichere Löschung von Daten sicherzustellen.	Kapitel 4	☐	☐
17.	Fenster und Türen sind zu verschließen, wenn ein Büroraum nicht besetzt ist.	Kapitel 5	☐	☐
18.	Datenträger oder Dokumente mit schutzbedürftigen Daten, bspw. aus dem Meldewesen, müssen weggeschlossen werden können.	Kapitel 5	☐	☐
19.	In Büroräumen mit Publikumsverkehr sind Diebstahlsicherungen zum Schutz von IT-Geräten einzusetzen.	Kapitel 5	☐	☐
20.	Bei mobilen Arbeitsplätzen (bspw. bei der Arbeit mit dem Notebook außerhalb der Büroräume) ist die Bildschirmsperre am Gerät einzurichten.	Kapitel 6	☐	☐
21.	An mobilen Arbeitsplätzen dürfen dienstliche Unterlagen und Geräte nicht unbeaufsichtigt bleiben.	Kapitel 6	☐	☐
22.	Der Zugriff von einem Laptop von außerhalb auf das interne Netz darf nur verschlüsselt, SSL/TLS oder VPN, erfolgen.	Kapitel 6	☐	☐
23.	Bei allen Mobiltelefonen/Smartphones/Tablets usw. ist die Eingabe der Geräte-PIN zu aktivieren.	Kapitel 7	☐	☐
24.	Vertrauliche Daten dürfen auf Mobiltelefonen/ Smartphones/Tablets usw. grundsätzlich nur verschlüsselt gespeichert werden.	Kapitel 7	☐	☐
25.	Das Senden von vertraulichen Daten ist nur über gesicherte, von kirchlichen Organisationen bereitgestellte Transportwege erlaubt. Insbesondere Skype, Whatsapp oder private E-Mail dürfen dafür nicht genutzt werden.	Kapitel 7	☐	☐
26.	Bei der Nutzung eines WLAN ist das Verschlüsselungsverfahren WPA2 einzusetzen.	Kapitel 8	☐	☐
27.	Voreingestellte Passwörter für ein WLAN sind vor Inbetriebnahme zu ändern.	Kapitel 8	☐	☐

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.

Ergänzende Hinweise

Kapitel 1: Sensibilisierung der Mitarbeitenden

Besonders wichtig ist die Sensibilisierung aller relevanten Mitarbeitenden (Personen, die Zugang zur EDV in der kirchlichen Stelle haben, bspw. in der Kirchengemeinde). 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.

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

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

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.

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.

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

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

Kapitel 2: 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 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.

Kapitel 3: 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).

Kapitel 4: 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.
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.

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.

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.

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.

Kapitel 5: 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.

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.

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

Kapitel 6: 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.

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

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

Kapitel 7: Mobiltelefon / Smartphone / Tablets

Mobiltelefone bzw. Smartphones und Tablets 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.

Kapitel 8: 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.