DER DATENSCHUTZBEAUFTRAGTE
FÜR KIRCHE UND DIAKONIE

Datenschutzaufsichtsbehörde gemäß Kapitel 6 DSG-EKD für:

Ev.-Luth. Landeskirche Sachsens
Evangelische Landeskirche Anhalts
Diakonisches Werk der Ev.-Luth. Landeskirche Sachsens e.V.
Diakonisches Werk Evangelischer Kirchen in Mitteldeutschland e.V.

Datenschutzbeauftragter
Herr Pierre Große

Reichenbrander Str. 4
09117 Chemnitz

Tel.: 0351 4692-460
Fax: 0351 4692-469

Datenschutzbeauftragter@evlks.de

Arbeitshilfe:

Umgang mit E-Mails

Aktenzeichen:
ARH.004.2022.01

Datum:
25.01.2022

1. Email eine offene Postkarte - mögliche Abhilfen

Eine E-Mail ist für Empfänger und auf ungeschützten Transportwegen ebenso leicht lesbar, wie eine Postkarte, hat aber den Charakter eines Briefes – muss geöffnet werden! Der Inhalt einer E-Mail ist ohne zusätzliche Vorkehrungen grundsätzlich nicht gesichert und alles, was darin steht, ist für jeden lesbar und veränderbar. Schützenswerte Daten, zu denen auch sensible *bzw.* personenbezogene Daten gehören, dürfen deshalb nicht unverschlüsselt per E-Mail versendet werden. Verschlüsselung der E-Mail Inhalte stellt sicher, dass nur befugte Empfänger die Inhalte einer E-Mail zur Kenntnis nehmen können.

Die Kommunikation per E-Mail bedarf mindestens einer Transportverschlüsselung. In diesem Fall wird mittels einer entsprechenden Konfiguration bzw. Protokolls der Transportkanal verschlüsselt und verhindert das Mitlesen während des Datentransportes. Zugriff haben dann nur die Schlüsselinhaber des Empfängers und des Absenders. Von einer datenschutzrechtlich verantwortlichen Stelle wird erwartet, dass sie gemäß dem Stand der Technik eine transportverschlüsselte Übertragung von E-Mails sicherstellt.

Zusätzlich zur Transportverschlüsselung gibt es die Möglichkeit, den Inhalt einer E-Mail zu verschlüsseln. Es ist möglich, Dateianhänge, die mit einer E-Mail versendet werden sollen, selbst zu verschlüsseln und das Entschlüsseln und Öffnen derselben von der Eingabe eines Passwortes abhängig zu machen oder die ganze E-Mail z.B. per PGP/MIME (PGP/MIME – Wikipedia) oder S/MIME (S/MIME – Wikipedia) zu verschlüsseln.

Falls keine Verschlüsselung möglich ist, sollte bei der Übermittlung von vertraulichen bzw. personenbezogenen Daten grundsätzlich der „traditionelle“ Postweg verwendet werden.

Eine weitere Alternative zur sicheren Kommunikation sind geschützte Cloud-Systeme (übersetzt: Wolke), welche internetbasiert sicheren Speicherplatz zur Verfügung stellen können (z. B. die CN-Cloud der Landeskirche Sachsens). Mit Hilfe solcher Systeme können die zu kommunizierenden Daten, z. B. große Dateien, welche für den E-Mail Versand zu groß sind, zwischen Sender und Empfänger über passwortgeschützte Zugänge zum betreffenden Speicherplatz miteinander ausgetauscht werden.

2. Der offene Email-Verteiler – wie geht es besser

Einen offenen E-Mail-Verteiler nennt man die Verwendung von mehr als einer E-Mail Empfängeradresse in den Feldern „An:“ oder „Cc:“ einer E-Mail.

Offene E-Mail-Verteiler dürfen nur unter definierten Bedingungen verwendet werden. Arbeit- bzw. Dienstgeber sollten mittels verständlicher Richtlinien zur E-Mail-Nutzung ihre Beschäftigten entsprechend anleiten und unterstützen.

Um eine Veröffentlichung sämtlicher Empfänger einer E-Mail zu verhindern, sollte in jedem Fall die sogenannte Blindkopie-Funktion („Bcc“) des Adress- bzw. Empfängerfeldes genutzt werden, da dann die Empfänger-Adressen für alle Empfänger nicht sichtbar sind. Die Nutzung der Bcc-Funktion ist daher zwingend notwendig, vor allem wenn private E-Mail-Adressen unter den Empfängern sind bzw. deren privater oder beruflicher Charakter unklar ist.

Außerhalb der innerkirchlichen bzw. innerbetrieblichen E-Mail Kommunikation bzw. beruflich oder geschäftlich bedingten Kommunikation mit externen Partnern dürfen offene E-Mail-Verteiler nur bei nachweisbarer Einwilligung aller Empfänger der Mail verwendet werden, andernfalls liegt mangels einer gültigen Rechtsgrundlage gemäß § 6 Abs. 1 Nr. 2 i. V. m. § 5 Abs. 1 Nr. 1 bzw. für Beschäftigtendaten gemäß § 49 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz - DSG-EKD) eine Verletzung des Schutzes personenbezogener Daten vor, die gemäß § 32 DSG-EKD meldepflichtig sein kann.

E-Mail-Adressen sind personenbezogene Daten im Sinne des § 4 Nr. 1 DSG-EKD. Auch personalisierte E-Mail-Adressen von Dienststellen gehören zu den personenbezogenen Daten.

Ist der Fall eingetreten, dass eine E-Mail versehentlich mit mehreren Empfängern im Adressfeld oder als Kopie verschickt wurde, müssen Maßnahmen zur Schadensbegrenzung ergriffen werden. Es sollte unverzüglich der Vorgesetzte und der örtliche bzw. betriebliche Datenschutzbeauftragte informiert werden. Diese können dann gemeinsam mit der Dienststellenleitung über den weiteren Umgang mit den betroffenen Empfängern der E-Mail beraten und gegebenenfalls die Datenschutzaufsichtsbehörde einbeziehen.

Um das versehentliche Verwenden offener E-Mail-Verteiler zu verhindern, sollten geeignete technische und organisatorische Maßnahmen geprüft und umgesetzt werden. Ausgewählte E-Mail Clients bieten für die technische Administration die Möglichkeit, die Anzahl der Empfängeradressen für eine E-Mail einzuschränken.

Empfohlen wird der Einsatz technischer Maßnahmen, welche die Beschäftigten bei der sicheren E-Mail-Kommunikation entlasten und unterstützen. So können technische Lösungen automatisiert für die Gewährleistung einer qualifizierten Transportverschlüsselung als auch für eine Verschlüsselung von E-Mail-Inhalten und -Anhängen sorgen. Der Verzicht auf solche Hilfsmittel allein aus Kostengründen stellt nach dem heutigen Stand der Technik keinen verhältnismäßigen Umgang mit den drohenden Risiken durch das Weglassen der Verschlüsselung als wirksame Maßnahme dar.

3. Tipps für mehr Datenschutz im E-Mail-Verkehr:

- Versenden Sie keine sensiblen bzw. personenbezogenen Daten per Mail ohne geeignete Schutzmaßnahmen.
- Verschlüsselung macht E-Mails sicherer.

- Wählen Sie einen neutralen Betreff, der keine sensiblen Daten enthält.
- Überprüfen Sie die E-Mail-Adressen der Empfänger vor dem Absenden.
- Nutzen Sie bei mehreren E-Mail-Empfängern das Bcc-Adress-/Empfängerfeld.
- Prüfen Sie vor jedem E-Mailversand, ob die Empfänger befugt sind, die E-Mail zu bekommen.
- Setzen Sie technische Hilfsmittel ein, damit Empfänger, egal ob innerbetrieblich oder extern eine E-Mail nicht an Unbefugte weiterleiten können.

4. Gefahren durch Phishing-Mails und andere Schadprogramme

Leider gibt es beim Versand elektronischer Post zahlreiche Gefahren. Es kommt immer wieder zu Versuchen mit Hilfe von E-Mails und diverser Schadsoftware, IT-Systeme zu missbrauchen und zu beschädigen.

Wegen der Gefahren durch Viren, Phishing und Spam sollten entsprechende Sicherheitsvorkehrungen vorhanden sein, und zwar mindestens

- Virenschutzprogramme, die ein- u. ausgehende E-Mails auf Schadprogramme prüfen,
- Anti-Spam-Software, die unerwünschte E-Mails erkennt und aussortiert,
- Anti-Phishing-Software, die Angriffe abwehrt, bei denen der Benutzer mittels gefälschter E-Mails animiert wird, vertrauliche oder persönliche Daten preiszugeben und
- eine Firewall, die alle eingehenden Verbindungen filtert.

Spammer (gemeint sind Versender von so genannten SPAM-Mails) animieren mit vielen Tricks die Empfänger gefälschte E-Mails zu öffnen, die sogenannte Malware – das sind Schadprogramme – enthalten können. Sie verschicken verfälschte E-Mails und versuchen z. B. mit angehängten „Mahnungen“ oder „unbezahlten Rechnungen“ zu verunsichern und vertrauen darauf, dass die meisten Mail-Empfänger nachschauen wollen, worum es sich hierbei handelt und damit schnell Dateianhänge mit Malware öffnen und ihre IT-Systeme infizieren.

Eine weitere Methode zur Einschleusung von Malware ist die Nutzung von HTML als E-Mailansicht. Damit wird die E-Mail als Webseite betrachtet, die Verknüpfungen zu verseuchten Webseiten enthalten kann. Dadurch ist es möglich, Malware automatisch von anderen Webseiten herunterzuladen, ohne dass diese Webseiten besucht werden. Das bloße Öffnen der E-Mail genügt!

Neben Malware gibt es so genannte Phishing-Attacken. In diesem Fall haben es Kriminelle auf sensible Daten, wie z.B. Benutzernamen oder Passwörter abgesehen. Dabei werden Empfänger mittels gefälschter E-Mails auf gefälschte Webseiten gelockt und die Benutzer zur Eingabe sensibler Daten (Benutzername, Passwort, PIN) aufgefordert. Solche E-Mails heißen Phishing-Mails und die dazugehörigen gefälschten Webseiten Phishing-Seiten. Diese Phishing-Seiten sind besonders gefährlich, da sie sich kaum von der Original-Webseite unterscheiden und Spammer können so Zugangsdaten abgreifen und damit Missbrauch betreiben oder IT-Systeme mit Ransomware infizieren.

Viele Phishing-Mails lassen sich durch entsprechende Überwachungssysteme abfangen, aber auch das Sicherheitsbewusstsein der Mitarbeiter ist ein sehr wichtiger Faktor. Da das Internet ein weltweites Medium ist, das keiner generellen Regelung unterliegt, helfen keine nationalen

Bestimmungen zur Eindämmung dieser Gefahren. Die Verantwortung liegt bei den Empfängern bzw. Verantwortlichen selbst, geeignete Sicherheitsmaßnahmen zu treffen.

5. Bedingungen für die Geltung des Briefgeheimnisses für E-Maildaten

Der Schutz des Briefgeheimnisses in § 202 StGB ist nicht auf unverschlüsselte E-Mails (und Faxe) anwendbar, weil eine solche E-Mail mit ihren Daten ohne eine Verschlüsselung nicht als "verschlossenes" und "verkörpertes Schriftstück" im Sinne des Strafgesetzbuches angesehen werden kann.

Wird eine E-Mail einschließlich der Anhänge jedoch verschlüsselt, dann stellt das unbefugte Öffnen oder Brechen der Verschlüsselung einen Straftatbestand dar. Nach §§ 202a und 303a Strafgesetzbuch (StGB) greift der Schutz auch gegen das Ausspähen von (verschlossenen) Daten. Es wird bestraft, wer unbefugt einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück, welches nicht für ihn bestimmt ist, öffnet oder sich vom Inhalt des Schriftstücks ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft.

Darüber hinaus können weitere Straftatbestände erfüllt sein, wenn spezielle Geheimhaltungspflichten, wie z. B. ärztliche Schweigepflicht, Seelsorgegeheimnis bestehen. Daher besteht insbesondere für den Absender vertraulicher Nachrichten eine erhöhte Sorgfaltspflicht.

6. Rechtssicherheit von E-Mails – derzeitiger Rechts- und Technikstand

E-Mails können unter bestimmten Umständen als elektronische Erklärungen angesehen werden mit denen jemand eine Willenserklärung (§ 126a BGB) abgibt. Grundsätzlich können Willenserklärungen ohne Einhaltung einer bestimmten Form rechtswirksam abgegeben werden. Sie sind in der Regel rechtswirksam, wenn die Person des Erklärenden genannt ist und der Eingang der E-Mail beim Empfänger nachweisbar ist. Sollte jedoch per Gesetz das Erfordernis der Schriftform einer Willenserklärung festgelegt sein, bedarf es für die Willenserklärung per E-Mail zusätzlich einer qualifizierten elektronischen Signatur gemäß dem Signaturgesetz - SigG.

Willenserklärungen per E-Mail dienen zur Information oder veranlassen zu einem bestimmten Verhalten. Deshalb können z.B. auch Verträge durch eine in einer E-Mail enthaltenen Erklärung abgeschlossen, verändert oder aufgehoben werden. Ausnahmen gelten wie erwähnt bei formbedürftigen Verträgen (z.B. über Grundstücke, Wohnraummieten, Bürgschaft etc.).

Problematisch ist die Beweiskraft von E-Mails, da sie ohne Verschlüsselung und Signatur leicht verfälscht werden können. Lediglich E-Mails oder elektronische Dokumente mit qualifizierten elektronischen Signaturen sind als rechtssicher einzustufen. Aufgrund zahlreicher bestehender gesetzlicher Regelungen, die eine Aufbewahrungspflicht für E-Mails verlangen und nicht zuletzt um eventuellen Rechtsstreitigkeiten vorzubeugen, sollten bzw. müssen E-Mails entsprechend ihrem Inhalt geordnet und unveränderbar archiviert werden, damit sie innerhalb der gesetzlichen und betrieblichen Aufbewahrungsfristen sicher verfügbar sind.

7. Abwägungen Datenschutz und Datensicherheit von E-Mail mittels Risiko-Analysen

Der Datenschutz soll auch und gerade im Zusammenhang mit der Verwendung von E-Mail die beteiligten bzw. betroffenen Menschen vor einem übermäßigen Eingriff des Staates oder der Organisation (z. B. Dienstgeber) in ihre gesetzlich verankerten Grundrechte und ihre

Menschenwürde schützen. Dies gewährleisten zuerst die Regelungen in den §§ 5 und 6 bzw. speziell für Beschäftigte in § 49 DSG-EKD.

Die mit dem Datenschutz eng verbundene (technische) Datensicherheit thematisiert das Gesetz dadurch, dass gemäß § 27 DSG-EKD die verantwortliche Stelle verpflichtet ist, „… geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten …“.

Dies betrifft auch die E-Mail-Sicherheit einer Dienststelle. Gegebenenfalls sind die Risiken mittels einer Risikoanalyse zu bewerten und einzustufen. Dabei ist die Eintrittswahrscheinlichkeit und Schwere der Beeinträchtigung bei der Datenübermittlung zu analysieren und das Risiko für die Rechte und Freiheiten natürlicher Personen bei der Auswahl und Umsetzung technisch-organisatorischer Maßnahmen zu beurteilen. Bei einer Risikoanalyse wird objektiv festgestellt, welches Risiko die Datenverarbeitung in sich birgt und dementsprechend können Maßnahmen zur Risikominimierung getroffen werden. Die Eintrittswahrscheinlichkeit ist soweit zu reduzieren, dass durch diese Maßnahmen für die Dauer der Verarbeitung kein hohes Risiko vorliegt.

Das kirchliche Datenschutzmodell (https://www.kirchliches-datenschutzmodell.de/) und zahlreiche weitere öffentlich zugängliche Publikationen zur Durchführung von Risikoanalysen, Datenschutz-Folgenabschätzungen und die Auswahl geeigneter Maßnahmen helfen dabei.

Chemnitz im Januar 2022

Der Datenschutzbeauftragte für Kirche und Diakonie

Reichenbrander Str. 4, 09117 Chemnitz

Unabhängige Aufsichtsbehörde gemäß Kapitel 6 des Kirchengesetzes über den Datenschutz (DSG-EKD)

Quellen und Links:

Ist die Kommunikation per E-Mail wirklich unsicher? - datenschutz-notizen | News-Blog der datenschutz nord Gruppe

Datenschutz: Warum E-Mails wie Postkarten sind (letterxpress.de)

BSI - Verschlüsselt kommunizieren (bund.de)

Offener E-Mail-Verteiler ist ein datenschutzrechtlicher Verstoß (idealo.com)

Bußgeld für offenen E-Mail-Verteiler (rosepartner.de)

Problem offener E-Mail-Verteiler: Vorbeugung und Nachsorge (dr-datenschutz.de)

Gefahren durch E-Mails: SPAM, Phishing, Malware und Scam E-Mails (edv-lehrgang.de)

Typische E-Mail-Risiken und wie man diesen begegnet (computerweekly.com)

Rechtsrat : Ist eine E-Mail rechtswirksam? - WELT

E-Mails und Recht | esb Rechtsanwälte (kanzlei.de)

Sind Erklärungen per E-Mail rechtskräftig? Einfach erklärt - CHIP