Der Beauftragte für den Datenschutz
der Evangelischen Kirche in Deutschland

Handreichung: Verschlüsselte Versendung von Protokollen bei elektronischer Kommunikation mit Ehrenamtlichen

Metadaten:

Version:	1.1
Ausgabedatum:	12. Mai 2015
Status:	☐ in Bearbeitung ☐ in Abstimmung ☑ Freigegeben ☐ nur zum Gebrauch innerhalb des BfD EKD ☑ zum allgemeinen kirchlichen Gebrauch
Ansprechpartner juristisch:	Der Beauftragte für den Datenschutz der EKD Sandra Coors 0511/169335-13 Sandra.Coors@datenschutz.ekd.de
Ansprechpartner technisch:	Der Beauftragte für den Datenschutz der EKD Klaus Knief 0511/768128-14 Klaus.Knief@datenschutz.ekd.de

Der Beauftragte für den Datenschutz
der Evangelischen Kirche in Deutschland

Inhaltsübersicht

Einführung

Beim Versenden von Protokollen mit einer E-Mail zwischen Ehrenamtlichen und beruflich Mitarbeitenden stellt sich regelmäßig die Frage nach der Einhaltung des Datenschutzes und der Datensicherheit.

Ehrenamtliche Arbeit wird oftmals im privaten Umfeld und mit dem privaten Rechner erledigt. Auch bei ehrenamtlicher Tätigkeit in (Leitungs-)Gremien werden so (Sitzungs-)Protokolle gefertigt und dann elektronisch an andere Ehrenamtliche oder beruflich Mitarbeitende versendet. Doch auch der umgekehrte Fall, wenn beruflich Mitarbeitende Protokolle im beruflichen Umfeld erstellen und dann an Ehrenamtliche versenden, ist datenschutzrechtlich relevant. Häufig geht es dabei auch um die Verarbeitung von personenbezogenen Daten. Es muss daher sichergestellt werden, dass mit diesen Daten datenschutzkonform umgegangen wird. Unbefugte dürfen keinen Zugriff auf diese Daten erhalten.

Zunächst ist zu gewährleisten, dass auf einem privaten Rechner erstellte Dateien, die personenbezogene Daten beinhalten, sicher abgespeichert werden. Grundsätzlich ist eine externe Festplatte oder ein USB-Stick zu empfehlen, die nur für die ehrenamtliche Arbeit genutzt werden. So vermischen sich nicht die privaten Daten mit den dienstlichen Daten. Außerdem sollte diese Festplatte bzw. dieser USB-Stick verschlüsselt sein, so dass beim Verlust keine unberechtigten Dritte Zugriff auf die Daten erhalten.

Auch beim Versenden von personenbezogenen Daten per E-Mail ist Vorsicht geboten. Auch dabei muss sichergestellt werden, dass ein Zugriff von außen nicht möglich ist. Das Verschicken von personenbezogenen Daten in einer unverschlüsselten Datei im Anhang einer E-Mail kann gerade diesen Schutz nicht bieten. Auf eine E-Mail, und damit auch auf ihren gesamten Inhalt, kann beim Transport von außen zugegriffen werden. Deshalb wird die E-Mail oft mit einer Postkarte oder einem offenen Buch verglichen. Wer sie in die Hände bekommt, kann sie lesen. Durch die Verschlüsselung des Inhalts einer der E-Mail angehängten Datei (zum Beispiel einem Sitzungsprotokoll) wird sichergestellt, dass nur derjenige die Datei lesen kann, der den Schlüssel kennt. Die Datei wird vor dem Anhängen an die E-Mail verschlüsselt und erst dann versendet. Zum Entschlüsseln muss nach dem Herunterladen der Datei ein Kennwort eingegeben werden. Keinesfalls darf das Kennwort per E-Mail verschickt werden. Das Kennwort kann z. B. am Ende einer Sitzung mündlich mitgeteilt werden. Nach drei Monaten ist zu empfehlen, das Kennwort zu wechseln. Dasselbe Passwort während der ganzen Amtsperiode eines (Leitungs-)Gremiums zu nutzen, ist nicht empfehlenswert. Ältere Protokolle bleiben mit dem alten Passwort lesbar. Es bedarf einer Dokumentation der Passworthistorie. Wer Zugriff auf die Passwortliste hat, muss im Vorfeld festgelegt werden und gehört ebenfalls zur Dokumentation. Die Liste sollte sicher gelagert werden und regelmäßig von einer dazu beauftragten Person gepflegt werden. Bei dieser Person ist dann auch im konkreten Fall das aktuelle oder ein älteres Passwort zu erfragen.

Es ist darauf zu achten, dass ein sicheres Passwort gewählt wird. Dafür sind folgende Regeln zu beachten:

- ✓ Ein Passwort sollte mindestens 12 Zeichen umfassen.
- ✓ Es sollte aus Groß- und Kleinbuchstaben sowie Sonderzeichen (?!%+…) und Ziffern bestehen.
- ✓ Es sollte nicht in Wörterbüchern vorkommen.
- ✓ Es sollte nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern bestehen, also nicht asdfgh oder 1234abcd usw.
- ✓ Einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen (z. B. : $! ? #) am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen, ist nicht zu empfehlen.

Die Hinweise zur Passwortqualität stammen aus dem Internetauftritt „BSI für Bürger“ des Bundesamtes für Sicherheit und Informationstechnik. Dort sind auch weitere nützliche Tipps zum Thema Passwörter zu finden.[1]

Im Übrigen sind die landeskirchlichen Vorgaben zu beachten.

[1] https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html (05.05.2015)

Technische Anleitung zur Verschlüsselung von Dateien

Wenn Dateien verschlüsselt übertragen werden sollen, kann man diese mit dem Programm 7-Zip im Vorfeld verschlüsseln und nach dem Empfang wieder entschlüsseln. Die Schlüssel, also die Passwörter, dürfen aus Sicherheitsgründen nicht per E-Mail übertragen werden, sondern auf einem gesonderten Weg.
Bei der Auswahl des Verschlüsselungsverfahrens („Encryption method“) ist die höchste Verschlüsselung zu wählen: AES-256.

Beschaffung des Programms 7-Zip

Das Programm 7-Zip ist unter der Open Source Lizenz erschienen und kann kostenlos auf der Herstellerseite (www.7-zip.de) heruntergeladen werden.
Eine offizielle Version der portierbaren Version gibt es nicht. Allerdings stellt der Anbieter PortableApps eine Version unter dem Link http://portableapps.com/de/apps/utilities/7-zip_portable zur Verfügung. Generell ist anzumerken, dass Software immer nur von vertrauenswürdigen Quellen genutzt werden sollte.

Anleitung für eine installierte Version von 7-Zip

Verschlüsselung von Dateien

Die entsprechende Datei oder den Ordner markieren und anschließend die rechte Maustaste drücken. Anschließend öffnet sich das Kontextmenü, mit dem 7-Zip aufgerufen werden kann:

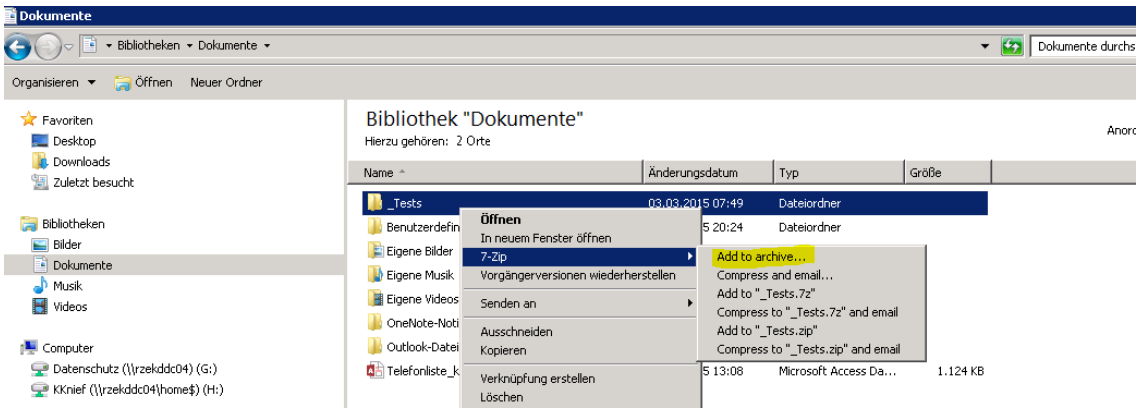

Abbildung 1: Hinzufügen von Dateien zu einem neuen Archiv

Über das Menü „Add to archive…“ oder „zu einem Archiv hinzufügen“ geben Sie das Passwort zur Verschlüsselung ein. Mit ok wird der Vorgang bestätigt und die Verschlüsselung vorgenommen.

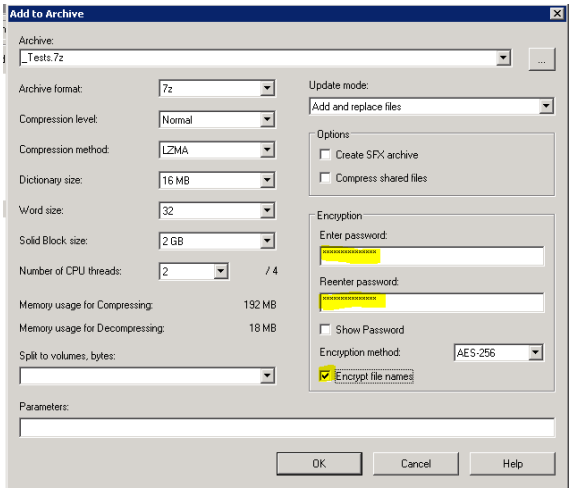

Abbildung 2: Setzen eines Passwortes zur Verschlüsselung des Archives

Entschlüsselung von Dateien

Über das Menü „Open archive“ oder „Öffnen“ wird die Datei entschlüsselt:

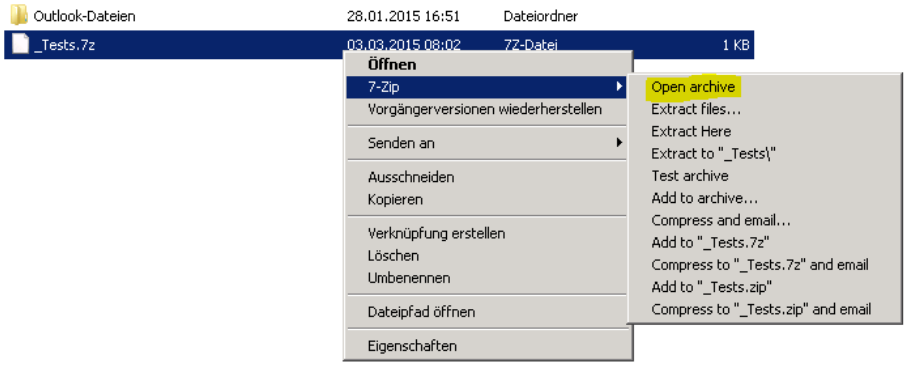

Abbildung 3: Das Archiv öffnen, um es zu entschlüsseln

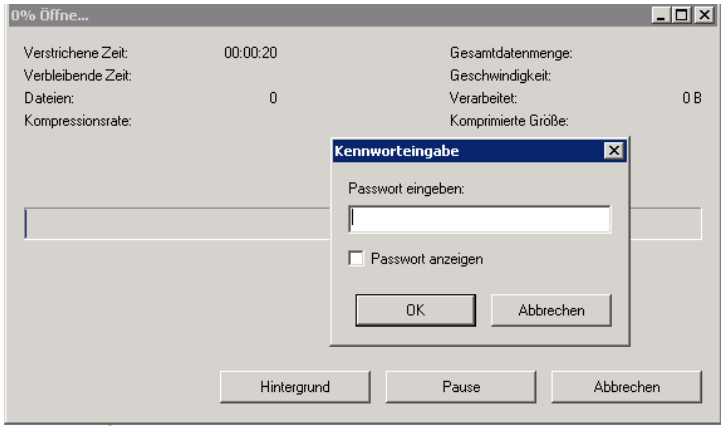

Abbildung 4: Automatische Abfrage des Passwortes findet statt

Über das Menü „Entpacken“ kann die Datei an den gewünschten Ort unverschlüsselt gespeichert werden:

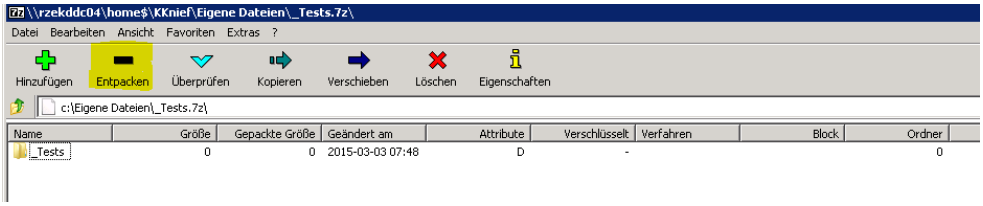

Abbildung 5: Der Inhalt kann anschließend an einem sicheren Ort gespeichert werden

Anleitung für eine portable Version von 7-Zip

Das Programm „7-Zip Portable“ kann ohne Installation aufgerufen werden. Über das Menü „Add“ oder „Hinzufügen“ erreicht man die Einstellungen für die Verschlüsselung (und Entschlüsselung):

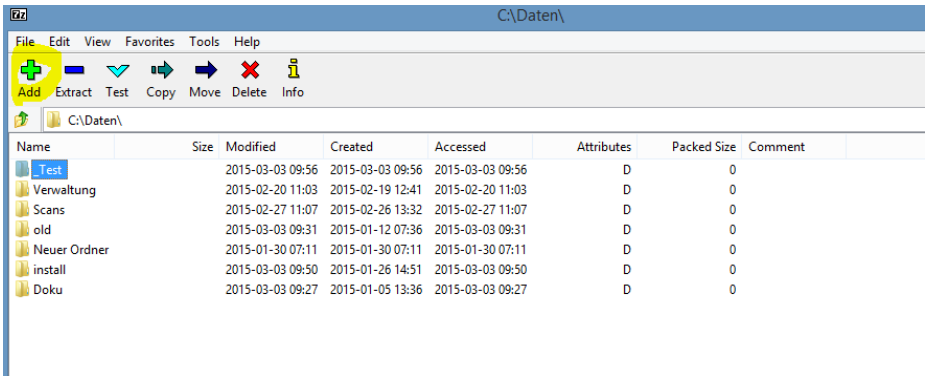

Abbildung 6: Durch das Menü hinzufügen können Daten hinzugefügt werden

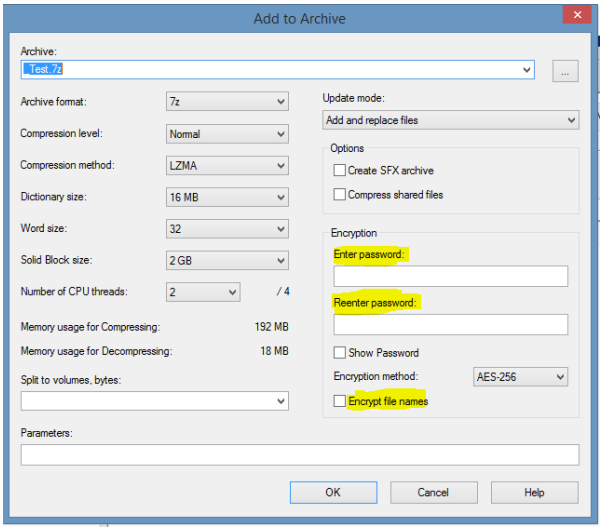

Abbildung 7: Durch das setzen eines Passwortes wird die Verschlüsselung aktiviert