Anlage zur Orientierungshilfe
„Datenschutz in der Mitarbeitervertretung"

Zum Thema: Einzelgeräte mit und ohne Netzwerk

Hier gibt es verschiedene Schutzmaßnahmen:

1. ***Schutz vor unbefugtem Zutritt zum Arbeitsplatz***

   a. Schließen Sie die Tür zu Ihrem Büro ab, wenn Sie es als letzter verlassen.

   b. Schließen Sie ebenfalls alle Fenster

2. ***Schutz vor unbefugtem Zugriff auf das Gerät***

   a. Aktivieren Sie den Kennwortschutz auf Ihrem Rechner, wenn Sie den Arbeitsplatz kurzzeitig verlassen

   b. Geben Sie Ihre Kennwörter nicht an Dritte weiter, auch nicht an Kollegen und an Vorgesetzte. Wenn Sie von Ihrem IT-Administrator ein neues Kennwort bekommen haben, dann ist dies unverzüglich zu ändern.

   c. Arbeiten Sie nicht als Administrator oder mit Administrator-Rechten auf dem PC, sondern stets mit einem nichtprivilegierten Benutzerkonto. Damit erschweren Sie es Schadprogrammen, unbemerkt Systemeinstellungen zu verändern.

   d. Falls der Verdacht besteht, dass die Daten unbefugten Dritten bekannt geworden sind, ist das Kennwort umgehend zu ändern und die zuständige IT-Administration zu informieren.

3. ***Schutz vor Missbrauch der Daten bei Diebstahl***

   a. Speichern Sie MAV-Daten verschlüsselt auf der lokalen Festplatte, um im Falle eines Diebstahls die Daten vor Missbrauch zu schützen. Mit Hilfe geeigneter Tools kann ein geschützter Container auf der Festplatte erstellt werden. Dafür ist das Windows-betriebssystemeigene Programm Bitlocker (sofern in Ihrer Lizenz enthalten) oder auch Software von Drittanbietern wie z.B. Veracrypt oder Cryptomator (beides freie Software) nutzbar.
   b. Wird der Container geöffnet, dann ist er als zusätzliches Laufwerk im Windows-Explorer nutzbar. Dateien können darin abgelegt, geändert oder gelöscht werden. Wird der Container geschlossen, dann sind die Daten verschlüsselt gespeichert und vor Zugriff gesichert.

4. Schutz vor Datenverlust

a. Sichern Sie lokal abgelegte Daten regelmäßig auf eine externe Festplatte oder einen externen USB-Stick. Hierfür sind verfügbare Backup-Tools oder Kopiertools wie z. B. FreeFileSync (freie Software) nutzbar.

b. Lagern Sie dieses externe Speichermedium – wenn möglich - räumlich getrennt in einem abschließbaren Büroschrank.

c. Achten Sie auch hier auf eine Verschlüsselung der Daten wie unter 3a.

5. Schutz vor Manipulation und Schadcode auf dem PC

a. Laden Sie keine Software oder Dateien aus dem Internet von unbekannten oder fragwürdigen Quellen herunter, da die Gefahr besteht, dass diese Dateien Schadcodebehaftet sind.

b. Konfigurieren Sie Ihre PC-Firewall so, dass ein Zugriff von außen auf Ihren Arbeitsplatz nicht möglich ist.

c. Nutzen Sie zum Schutz Ihres Arbeitsplatzes einen aktuellen Virenscanner. Dienstliche Arbeitsplätze im Kirchennetz der Landeskirche haben die Möglichkeit, einen zentral bereitgestellten Virenscanner zu nutzen.

Zum Thema: Internet/Intranet

Schutz vor unbefugtem Zugriff im Netzwerk

a. Wenn nicht alle Teilnehmer an das Kirchennetz angeschlossen sind, dann kann das Ablegen und der Austausch von Dokumenten wie z.B. Protokollen webbasiert in einem geschützten Intranet-Bereich vorgenommen werden. Ansonsten sollte ein Netzlaufwerk im LAN der Dienststelle genutzt werden.

b. Sollten sie Dokumente auf einem Cloudlaufwerk speichern, dann achten Sie darauf, dass diese verschlüsselt sind. Nutzen Sie nur Clouddienste, die Daten innerhalb der EU speichern. Keinesfalls sollten Cloudlaufwerke wie z.B. Dropbox oder Google Drive verwendet werden.

c. Nutzen Sie definierte kirchliche Plattformen wie intern-e, um Dokumente abzulegen.

d. Richten Sie geschützte und geschlossene Arbeitsgruppen ein, um den Teilnehmerkreis genau zu definieren.

Zum Thema: Nutzung von E-Mail

1. Bei der Nutzung von Email für die MAV kommt es auf eine strikte Trennung zwischen MAV-Mails und sonstigen Dienstmails an.

   a. Dafür ist es sinnvoll, wenn jedes MAV-Mitglied neben seinem persönlichen Dienstpostfach noch ein MAV-Postfach zur Verfügung gestellt bekommt, das ausschließlich für MAV-Angelegenheiten genutzt wird.

   b. Stellvertreterregelungen oder Mailweiterleitungen sollten stets nur zwischen MAV-Postfächern untereinander vorgenommen werden.

   c. Auch bei den MAV-Postfächern sind die Zugangsdaten geheim zu halten und auf keinen Fall an Dritte weiterzugeben.

2. Beim Versand von sensiblen Informationen ist im Wesentlichen zu unterscheiden, an welche Empfänger der Versand erfolgt.

   a. Erfolgt der E-Mail Austausch zwischen zwei Kommunikationspartnern, die eine „evlka.de" E-Mail Adresse besitzen, so können Sie davon ausgehen, dass die E-Mail Übertragung ausschließlich über verschlüsselte Leitungen des Kirchennetzes erfolgt und somit geschützt ist.

   b. Hat ein Kommunikationspartner keine „evlka.de" Adresse, so erfolgt der Versand höchstwahrscheinlich über das Internet. Von einem Schutz der Übertragung darf auf keinen Fall ausgegangen werden. In diesem Fall ist der Schutz der Informationen durch eine Verschlüsselung unabdingbar.

3. Der Gesamtausschuss der Mitarbeitervertretungen empfiehlt zurzeit für die Verschlüsselung von Anlagen das Tool Encrypto. Beachten Sie hierbei, dass der normale Nachrichtentext unverschlüsselt bleibt.

4. Die Landeskirche wird mittelfristig eine Mailverschlüsselungslösung etablieren, die den verschlüsselten Versand der gesamten Mail für Anwender in der Domain „evlka.de" ermöglichen wird.