Rundschreiben Nr. 1/2015 des Landeskirchenamtes an die Ev. Kirchenkreise – Kreiskirchenämter, Superintendentinnen und Superintendenten, Verbände kirchlicher Körperschaften, Ämter und Einrichtungen der Ev. Kirche von Westfalen betreffend kirchlicher Datenschutz: Hinweise zum Umgang mit Passwörtern[1]

Vom 2. Februar 2015 (Az.: 612.213/07)

Im Rahmen von Untersuchungen wurde festgestellt, dass die Anwenderinnen und Anwender zum Teil leichtfertig mit Benutzerkennung und Passwörtern umgehen und dadurch ein erhebliches Sicherheitsrisiko darstellen könnten. Wir haben die Hinweise zum Umgang mit Passwörtern aktualisiert und empfehlen, diese den Benutzerinnen und Benutzern der IT-Anwendungen bekanntzugeben oder in ihre Passwort-Richtlinie oder Dienstanweisung zu übernehmen.

Hinweise zum Umgang mit Passwörtern

Stand 27.01.2015

„Gute Passwörter sind das Eingangstor zur Informationssicherheit."

Ein nicht zu unterschätzendes Sicherheitsrisiko stellen die Anwenderinnen und Anwender dar. Untersuchungen haben gezeigt, dass einfache Passwortvarianten bevorzugt werden, wie „123456", „meinpc", „abc123", „hallo", „passwort" oder einfach der eigene Name, der des Haustieres oder das Geburtsdatum. Hackern wird es leicht gemacht, Passwörter auszuspähen, in dem sie vollautomatisch eine Vielzahl möglicher Zahlenkombinationen ausprobieren oder ganze Wörterbücher für den Angriff mit Hochleistungs-PCs nutzen.

Auch kommt es immer wieder vor, dass Kolleginnen und Kollegen oder sogar Vorgesetzte die Benutzerkennung und das Passwort für Vertretungszwecke erhalten oder dass mehrere Mit-arbeitende für ein DV-Programm eine gemeinsame Benutzerkennung und ein gemeinsames Passwort verwenden. Datenschutzrechtlich sind beide Varianten nicht zulässig. Denn nur die Vergabe individueller Benutzerkennungen und individueller Passwörter erfüllt die Anforderungen des Datenschutzrechts (siehe Anlage zu § 9 Abs. 1 DSG-EKD[2]).

1 Redaktioneller Hinweis: Am 24. Mai 2018 ist das neu gefasste EKD-Datenschutzgesetz vom 15. November 2017 (Nr. 850) in Kraft getreten. Es wird zurzeit geprüft, ob und inwieweit eine Aktualisierung der Regelungen des Rundschreibens an das neue kirchliche Datenschutzrecht erforderlich ist.

2 Nr. **850 Archiv-1**.

Damit den Passwörtern ein starker Schutz zukommt, sind richtig gute Passwörter zu verwenden. Die Passwörter sind immer geheim zu halten und regelmäßig zu ändern!

Folgende Hinweise sind zum Umgang mit Benutzerkennungen und Passwörtern zu beachten:

1. Es sind **individuelle Benutzerkennungen** und **individuelle Passwörter** zu verwenden.
2. Ein gutes Passwort sollte **mindestens 10, besser 12 Zeichen** lang sein.
3. Das Passwort sollte aus **Groß- und Kleinbuchstaben** sowie **Sonderzeichen und Ziffern** bestehen.
4. **Triviale Passwörter sind zu vermeiden.** Tabu sind Namen von Familienmitgliedern, des Haustieres, der besten Freundin, des Lieblingsstars oder Geburtsdaten u.s.w.
5. Das Passwort sollte **nicht in einem Wörterbuch vorkommen**. Zu vermeiden sind auch gängige Varianten oder Wiederholungs- oder Tastaturmustern, also nicht „asdfgh“ oder „1234abcd“ u.s.w.
6. Für ein **gutes Passwort** lohnt es sich, kreativ zu werden. Um ein komplexes und dennoch leicht zu merkendes Passwort zu konstruieren, empfiehlt sich ein Merksatz als Esels-brücke. Dabei denkt sich die Nutzerin oder der Nutzer einen Satz aus und benutzt von jedem Wort beispielsweise nur den ersten Buchstaben. Anschließend verwandelt man bestimmte Buchstaben in Zahlen oder Sonderzeichen. So wird z.B. aus dem Merksatz „Zum Datenschutz gehört ein gutes Passwort, um unberechtigte Zugriffe zu verhindern“ das Passwort „ZDg1gP@uuZz8!“.
7. **Passwörter sind regelmäßig zu ändern.** Am Besten legen Sie Wiedervorlagetermine an, die Sie in bestimmten Zeitabständen an die Passwortänderung erinnert. Spätestens nach 1 Jahr ist die Änderung des Passwortes durchzuführen. Für mehrere DV-Programme sind unterschiedliche Passwörter zu verwenden. Problematisch ist die Gewohnheit, einheitliche Passwörter für viele verschiedene Zwecke zu verwenden. Denn gerät das Passwort einer einzelnen Anwendung in falsche Hände, sind auch die anderen Anwendungen nicht mehr geschützt.
8. **Voreingestellte Passwörter in DV-Programmen sind zu ändern**. Bei vielen DV-Produkten werden bei der Installation oder im Auslieferungszustand in den Accounts leere Passwörter oder allgemein bekannte Passwörter „0000“ verwendet. Diese sollten von der Nutzerin oder dem Nutzer schnell geändert werden.
9. Hat die IT-Administration Ihnen ein Passwort eingerichtet, so haben Sie dieses **„Start-Passwort“** bei der ersten Anmeldung zu ändern.
10. Lassen Sie sich beim **Eintippen des Passworts nicht über die Schulter schauen. Es ist umgehend zu ändern**, wenn der Verdacht besteht, dass es einem Dritten bekannt wurde.

11. **Teilen Sie niemals Dritten** (auch nicht den IT-Administratoren) **ihr Passwort mit**. IT-Administratoren haben grundsätzlich alle für Ihre Arbeit notwendigen Rechte und sind nicht auf die Mitteilung Ihres Passwortes angewiesen.
12. Bei Abwesenheit ist der **Bildschirmschoner** zu starten und **mit Kennwort** zu sichern. Bei den gängigen Betriebssystemen haben die Nutzerinnen und Nutzer zusätzlich die Möglichkeit, den Bildschirm nach einer gewissen Zeit der Inaktivität automatisch sperren zu lassen. Die Entsperrung erfolgt erst nach Eingabe des korrekten Passwortes. Damit wird verhindert, dass Dritte sonst bei vorübergehender Abwesenheit Zugang zum PC, den DV-Programmen und Daten erhalten.
13. **Passwörter sollten niemals per Zettel am Bildschirm oder auf dem Schreibtisch kleben oder unter der Tastatur liegen oder unverschlüsselt auf dem PC abgelegt werden**. Wer sich Passwörter notieren will, sollte sie stattdessen auf Papier unter Verschluss halten. Am besten tragen Sie den Zettel immer bei sich, z. B. in Ihrem Portemonnaie.

    Sie können Passwörter auf dem Rechner in einer verschlüsselten Datei ablegen. Fragen Sie ggf. Ihre IT-Administration nach einem Passwort-Verwaltungsprogramm, wie z. B. KeePass. Diese Programme können neben der Passwort-Verwaltung auch starke Passwörter unter Berücksichtigung der o. a. Hinweise generieren. Das hat den Vorteil für Sie, dass Sie sich nur noch ein gutes Masterpasswort überlegen und merken müssen.

Hinweise für die IT-Administration:

1. Die Einstellungen des DV-Programms sollten vorsehen, dass nach mehreren fehlerhaften Anmeldeversuchen unter derselben Benutzerkennung diese für die weitere Benutzung gesperrt wird.
2. Um zu verhindern, dass die Benutzerin oder der Benutzer das gleiche Passwort beim Wechsel direkt wieder einstellt oder zwei oder mehr Passwörter im Wechsel nutzt, sollte system- bzw. programmseitig eine Passworthistorie mit mindestens der letzten vier benutzten Passwörter aktiviert sein.
3. System- oder programmseitig sollten möglichst Trivialpasswörter erkannt und abgelehnt werden. Die Liste von Trivialpasswörtern ist regelmäßig zu ergänzen.