Sicherheit

Allgemeine Informationen

Da das Intranet als ein virtuelles Netz die öffentlichen Telefonleitungen nutzt, müssen besondere Datensicherungssysteme eingebaut werden. Denn auf den gleichen Leitungen laufen Telefongespräche, Fax- und Datenübertragungen (auch Internetverkehr).

Gegenüber dem Internet als möglicher Zugriffsmöglichkeit auf die Intranetdaten muss es also eine Abschirmung geben. Dies geschieht mit Hilfe einer Firewall (- eine elektronische Schutzmauer gegen Hacker, Viren oder andere "Neugierige"). Der Zugang zum Intranet der EKHN wird also nur denjenigen möglich sein, die sich angemeldet und eine Nutzerkennung und ein Passwort erhalten haben. Beide dürfen selbstverständlich keinesfalls weitergegeben werden.

Da ein Intranet nur Sinn macht, wenn den Nutzenden auch der Internetzugang ermöglicht wird, sorgt die Firewall dafür, dass man vom Intranet der EKHN in das Internet kommt, aber als Nichtberechtigte nicht vom Internet in das Intranet.

Auch E-Mails aus dem world wide web werden zunächst in der Firewall auf eventuell enthaltene Viren oder Hackerangriffe untersucht. Erst wenn sie "sauber" sind, werden sie an Adressen im Intranet weitergeschickt.

Für die Nutzenden im Intranet ergibt sich dadurch die Möglichkeit, in einem geschützten Raum Daten und Informationen auszutauschen, ohne dass andere darauf zugreifen oder sie sogar verändern könnten.

Datenschutzrechtliche Bestimmungen

Datenschutzrechtliche Bestimmungen sind auch beim Einsatz von Computern zu beachten. Personen, die Zugriff auf die Datenbestände haben sollen, müssen durch eine schriftliche Erklärung verpflichtet werden (gemäß § 6 des Kirchengesetzes über den Datenschutz der EKD [Amtsblatt der EKHN 1994, S. 160] in Verbindung mit § 2 Abs. 4 der Datenschutzverordnung [Amtsblatt der EKHN 1979, S. 16 ff.]). Entsprechende Merkblätter und Muster-Verpflichtungserklärungen sind bei jedem Rent- und Gemeindeamt und bei der Kirchenverwaltung erhältlich.

Werden personenbezogene Daten automatisiert verarbeitet Maßnahmen zu treffen, die geeignet sind, ...

- ... Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren **(Zugangskontrolle)**;
- ... zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können **(Datenträgerkontrolle)**;
- ... die unbefugte Eingabe in den Speicher sowie die Löschung gespeicherter personenbezogener Daten zu verhindern **(Speicherkontrolle)**;
- ... zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können **(Benutzerkontrolle)**;
- ... zu gewährleisten, dass die zur Benutzung Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können **(Zugriffskontrolle)**;
- ... zu gewährleisten, dass überprüft werden kann, an welche Stelle personenbezogene Daten durch Einrichtungen der Datenübertragung übermittelt werden **(Übermittlungskontrolle)**;

- ... zu gewährleisten, dass überprüft werden kann, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind **(Eingabekontrolle)**;
- ... zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden **(Auftragskontrolle)**;
- ... zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können **(Transportkontrolle)**
- ... die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird **(Organisationskontrolle)**.

Darüber hinaus legt § 3 der EDV-Verordnung der EKHN (Amtsblatt der EKHN 1990, S.220) fest, dass private EDV-Geräte und Programme nicht zur Verarbeitung von Meldewesen-, Personalwesen- und Finanzwesen-Daten sowie sonstiger dienstlicher personenbezogener Daten eingesetzt werden dürfen.

Datensicherheit

Das Sicherheitskonzept für das Intranet der EKHN sieht in diesem Zusammenhang folgende Regeln verbindlich vor:

- Das Intranet der EKHN wird geschützt durch sogenannte Paketfilter und ein differenziertes Firewall-System.
- Die Einwahl erfolgt über ein Kennwort mit mindestens sechs Stellen. Die Kennwortgültigkeit wird auf maximal 3 Monate begrenzt. Kennwörter müssen verschlossen aufbewahrt werden und dürfen nicht an Dritte weitergegeben werden.
- Die Nutzung des E-Mail-Systems für private Zwecke ist in Einzelfällen zulässig, soweit dadurch betriebliche Abläufe und arbeitsvertragliche Pflichten nicht beeinträchtigt werden.
- Das E-Mail-System kann nicht zwischen privater und dienstlicher Nutzung unterscheiden. Um dem Fernmeldegesetz Rechnung zu tragen, sind der Empfang und das Versenden von privaten E-Mails nur dann zulässig, wenn die Beschäftigten sich damit einverstanden erklären, dass die Regelungen für dienstliche E-Mails auch auf private E-Mails angewandt werden.
- Anlagen (sog. Attachements) dürfen nur dann geöffnet werden, wenn Sie vorab auf Viren überprüft wurden. E-Mails unbekannter Herkunft sowie Anlagen privater E-Mails dürfen nicht geöffnet werden.
- Eine Nutzung des Internet für private Zwecke ist in Einzelfällen zulässig, soweit dadurch betriebliche Abläufe und arbeitsvertragliche Pflichten nicht beeinträchtigt werden.
- Das E-Mail-, Intranet- und Internet-System darf nicht für rechtswidrige, rassistische, gewaltverherrlichende, pornografische, diskriminierende oder gegen die Sicherheit der EKHN und ihrer Beschäftigten gerichteten Aktivitäten verwendet werden.
- Downloads (Übertragung von Dateien vom dem Internet auf den Computer) sind nur gestattet, wenn sie dienstlich notwendig sind und während des Herunterladens auf Viren überprüft wurden. Downloads für private Zwecke sind nicht gestattet.

Für die Mitarbeiterinnen und Mitarbeiter werden die Verhaltens- und Sicherheitsregeln im Zusammenhang mit der Nutzung des Internets und der E-mail-Funktionen über Dienstvereinbarungen, Geschäftsanweisungen und eine Novellierung der EDV-Verordnung verbindlich geregelt. Es ist vorgesehen, Mitarbeiterinnen und Mitarbeiter über eine schriftliche Erklärung, ähnlich der Datenschutzerklärung, zu verpflichten.