Verfasser: DI Claudia Springer-Knam
Stand Februar 2003

Datensicherheitsmaßnahmen für Web-Anwendungen

Generelle Bestimmungen

Zur Gewährleistung einer sicheren elektronischen Kommunikation zwischen der Steirischen Landesverwaltung und ihren Kommunikationspartnern sind Sicherheitsmaßnahmen auf mehreren Ebenen zu treffen. Die Einhaltung dieser Bestimmungen ist Voraussetzung für einen ordnungsgemäßen Betrieb und daher verpflichtend für alle Teilnehmer.

Die unter dem Punkt „Allgemeine Sorgfaltspflicht“ beschriebenen Maßnahmen gelten für alle Benutzer, unabhängig von ihrer Funktion.

Allgemeine Sorgfaltspflicht

Benutzerkonten und Passworte

Die Anlage von Benutzerkonten (Benutzerregistrierung) in den einzelnen personalführenden Stellen erfolgt **durch die jeweils nominierten Benutzerverwalter**. Beim Einrichten der Benutzerkonten wird ein **vereinbartes Standard-Passwort** vergeben, welches **beim ersten Anmeldevorgang vom berechtigten Benutzer zu verändern** ist. Es ist darauf zu achten, dass diese Passwort-Änderung noch am selben Tag, jedenfalls aber so bald wie möglich erfolgt.

Benutzerkonten sind **personenbezogen**, daher darf nur der Eigentümer das jeweilige Konto benutzen. Die Benutzer dürfen das Passwort **unter keinen Umständen** anderen Personen **bekannt geben**. Eine schriftliche Fixierung ist nur zulässig bei versiegelter Aufbewahrung in einem Schließfach, wobei die Eröffnung des Siegels zu dokumentieren ist.

Weiters gelten die folgenden Bestimmungen für Passworte:

- Ein **Passwort** muss aus **mindestens 6 Zeichen** bestehen und muss nach **spätestens 180 Tagen** umgesetzt werden. Sollte der Verdacht bestehen, dass das Passwort auch Personen außerhalb des berechtigten Personenkreises bekannt ist, so ist das Passwort auch vor Ablauf dieser Frist sofort zu ändern.
- Die Verwendung von **Trivial-Passwörtern** ist unbedingt zu **unterlassen**. (Trivial-Passwörter sind solche Passwörter mit spezieller Bedeutung, welche leicht auch von Außenstehenden erraten oder bestimmt werden können. Also z.B. Namen (eigene, aus der Familie, von Prominenten), Geburtsdaten, Firmen- und Abteilungsbezeichnungen, Kfz-Kennzeichen usw.. Ebenfalls in diese Gruppe fallen Standardausdrücke wie etwa TEST, SYSTEM, Tastatur- und Zeichenmuster, wie ABCDEF, QWERTZ, 123456,...)

- Innerhalb eines Passwortes sollte mindestens 1 Zeichen verwendet werden, das kein Buchstabe ist (**Zahl oder Sonderzeichen**).
- Ganz allgemein ist darauf zu achten, dass die **Eingabe** des Passwortes **unbeobachtet** erfolgt.
- Passwörter dürfen **nicht** auf programmierbaren Funktionstasten **gespeichert** werden.

Soweit es das jeweilige Betriebssystem zulässt, ist die Einhaltung dieser Richtlinien durch entsprechende Einstellungen des Betriebssystems sicherzustellen.

Eine fünfmalige Fehleingabe des Passwortes führt zur Sperrung der Zugangsberechtigung, welche nur durch den Rechteverwalter der Organisationseinheit wieder aufgehoben werden kann.

Virenschutz

Viren, ebenso wie Trojaner, Würmer u.a.m., sind Programme, die verdeckte Funktionen enthalten und damit durch Löschen, Überschreiben oder sonstige Veränderungen **unkontrollierbare Schäden an Daten und Programmen** anrichten können. Um diese Schäden und die damit verbundenen oft erheblichen Kosten und Aufwendungen zu vermeiden, sind insbesondere die **folgenden vorbeugenden Maßnahmen** zu treffen:

- Einsatz eines markgängigen **Anti-Viren Programms**
- **Regelmäßiges Update** der Virendatenbank.
- **Überprüfung** aller ein- und ausgehenden **Datenträger**.

Zugriffsschutz und Raumsicherheit

Zusätzlich zu den schon genannten Maßnahmen ist es notwendig, den Zutritt zu den Räumen und Geräten zu regeln, in denen sich Kommunikationsendpunkte (also in der Regel PCs) befinden.

Folgende Maßnahmen werden dringend empfohlen:

- **Verbindungen** sind zu **trennen**, sobald sie nicht mehr benötigt werden.
- Bei **kurzer Abwesenheit** ist **immer ein Bildschirmschoner** mit **Passwortschutz** zu verwenden (**Wartezeit 5 Minuten).**
- Bei **längerer Abwesenheit** ist der PC **/** die Workstation **niederzufahren.**
- **Räume** sind beim Verlassen **abzusperren**, wo immer das möglich ist.
- **Bildschirme** sind **so aufzustellen**, dass **keine unbefugte Einsicht möglich** ist.
- **Datenträger**, **Ausdrucke** sind vor Einsichtnahme zu **schützen**.