Artikelserie Kommunalsoftware auf dem Prüfstand[1]

(Auszug aus der Veröffentlichung im OKKSA-Newsletter Nr. 17 vom 17.04.08)

Teil 7: Passwortrestriktionen - darf Sicherheit erzwungen werden? (von Dr. Uwe Schwochert)

Zugriffschutz und Passwortvergabe sind aus Anwendersicht zunächst vor allem notwendige Übel. Dabei darf aber nicht vergessen werden, dass sich hier eine ganze Reihe von Anforderungen an das Softwareprodukt ergeben, die bei seiner Beschaffung berücksichtigt werden müssen.

Aus der Grundforderung der differenzierten Aufgabenbearbeitung ergibt sich zunächst die allgemeine Notwendigkeit einer wirksamen Zugriffskontrolle auf fachlich eingesetzte Programme.
Mit dem Kriterium

[FÜ4.1] *Das Programm stellt Zugriffskontrollmechanismen wie beispielsweise die Passwortvergabe zur Verfügung und gewährleistet so einen kontrollierten Zugang zu den gespeicherten Daten durch identifizierte und authentifizierte Benutzer.* (MUSS-Kriterium)

wird dieser allgemeine Anspruch formuliert. Im Weiteren wird vor allem der passwortorientierte Zugriffsschutz (als verbreitetste Variante) betrachtet und mit mehreren Einzelforderungen konkretisiert:

[FÜ4.2] *Programmseitig ist gewährleistet, dass ein Passwort bei der Eingabe nicht am Bildschirm angezeigt wird.* (MUSS-Kriterium)
[FÜ4.4] *Bei der Passworteinrichtung bzw. -änderung stellt das Programm zwei getrennte Eingabefelder zur Passwortwiederholung bereit und überprüft deren Übereinstimmung.* (MUSS-Kriterium)
[FÜ4.5] *Passwörter werden im System verschlüsselt abgelegt und sind gegen unbefugte Schreib- und gegen unbefugte Lesezugriffe geschützt.* (MUSS-Kriterium)
[FÜ4.6] *In vom Programm erzeugten Protokollen oder Dateien dürfen Passwörter nie in Klarschrift erscheinen.* (MUSS-Kriterium)

Unterschätzt wird allerdings häufig die Verantwortung, die der Benutzer bezüglich seines eigenen Passworts hat. So soll er es insbesondere selbst ohne fremde Hilfe jederzeit ändern können.

[FÜ4.3]
Das Programm stellt sicher, dass jeder Nutzer ein eigenes Passwort hat und sein Passwort selbst vergeben kann. (MUSS-Kriterium)

So weit so gut. Um dem Risikopotential einer missbräuchlichen Programmbenutzung sowohl aus Datenschutz- als auch aus Finanzsicht zu begegnen, sind diese Anforderungen allerdings nicht ausreichend. So muss es möglich sein, auch Versuche einer **missbräuchlichen Programmbenutzung zu erkennen** und darauf zu reagieren:

[FÜ4.7] *Das Programm gestattet die Einstellung von Zugangsrestriktionen als Reaktion auf mehrfache Falscheingaben von Passwörtern.* (MUSS-Kriterium)
[FÜ4.8] *Nicht erfolgreiche Anmeldungen werden übergreifend und benutzerbezogen protokolliert.* (MUSS-Kriterium)

[1] Hinweis: Die in der Artikelserie genannten Kriterien stammen aus der aktuellen Fassung des "OKKSA Anforderungskatalogs für Fachprogramme in der Öffentlichen Verwaltung - Teilbereich Fachübergreifende Programmanforderungen", Version 3.1

[FÜ4.9] *Die Login-Information zur letzten Programmnutzung wird dem Benutzer automatisch bei Anmeldung im Programm angezeigt.* (KANN-Kriterium)
[FÜ4.10] *Die Login-Information zum letzten nicht erfolgreichen Versuch einer Anmeldung wird dem Benutzer bei der aktuellen Anmeldung angezeigt.* (KANN-Kriterium)

Wichtig ist dabei natürlich auch, dass die entsprechenden Protokolle selbst vor unbefugtem Zugriff geschützt sind.

Das größte Risiko kommt allerdings weniger durch mangelnde technische Sicherheitsmechanismen. **Größter Schwachpunkt sind erfahrungsgemäß Programmbenutzer**, die nachlässig mit diesen Mechanismen umgehen.

Aus Sicht der OKKSA-Kriterienkataloge ist der Anwender zunächst nicht selbst Prüfgegenstand. Trotzdem kann dieses Risiko beim verantwortungsbewussten Verfahrenseinsatz nicht ignoriert werden. Nur vor Ort kennt man die Benutzer, nur vor Ort kann deren Sicherheits- und Verantwortungsbewusstsein eingeschätzt werden.

Da das **"benutzerbezogene Sicherheitsniveau"** objektiv unterschiedlich hoch sein kann, müssen die Programme eine Robustheit auch gegenüber dem "Worst Case" besitzen. Konkret muss es eine Vorstellung darüber geben, wie fahrlässig Anwender mit den Zugriffsmechanismen umgehen könnten.
Resultat dieser Betrachtung sind Mechanismen, die einen fiktiv entmündigten Programmbenutzer vor seiner eigenen Unbedarftheit schützen sollen:

[FÜ4.11] *Die technisch einstellbare Mindestlänge des Passwortes beträgt mindestens 6 Stellen über den gesamten Zeichenvorrat.* (MUSS-Kriterium)
[FÜ4.12] *Das Programm kann neue Passwörter, die nicht aus einem alphanumerischen Zeichenmix mit mindestens einem Sonderzeichen bestehen, abweisen.* (KANN-Kriterium)
[FÜ4.13] *Im Programm kann eingestellt werden, dass der Benutzer sein Passwort regelmäßig (z. B. spätestens aller 90 Tage) wechseln muss.* (MUSS-Kriterium)

Das besondere an diesen Kriterien ist, dass sie nicht regeln sollen, wie sehr der Anwender tatsächlich bevormundet wird. Hier gibt es Freiheitsgrade, die in Anbetracht des tatsächlichen Missbrauchsrisikos vor Ort (welches wesentlich auch vom Einsatzzweck des Programms abhängen wird) eingestellt werden sollen. So muss zum Beispiel für ein Finanzprognosetool zur Liquiditätsüberwachung nicht unbedingt ein 12stelliges Passwort mit Zwang zum vierteljährlichen Wechsel eingestellt werden.

Andererseits wird der sicherheitsbewusste Anwender aber auch erkennen, dass keine der Anforderungen aus der Luft gegriffen ist und eine einstellbare Überwachung sogar als Nutzungsunterstützung wahrgenommen werden kann. Ein Hinweis auf ein zu kurzes oder zu triviales Passwort kann ihm helfen, Sicherheitsaspekte bewusster wahrzunehmen und sich damit auch der Verantwortung der eigenen Tätigkeit bewusst zu werden.

Nächster Teil der Serie:
Keiner für alles? Filigrane Zugriffsrechte als Praxisbremse.