LSI-Info T#02

SICHERHEITSKRITERIEN FÜR KOMMUNALE FACHANWENDUNGEN

Version 1.0 vom: 11.02.2020

Management Summary

In der kommunalen Landschaft finden sich, bedingt durch die Aufgabenvielfalt der kommunalen Verwaltung, eine Vielzahl an Fachanwendungen. Diese sollen die Verwaltung effizienter und schlanker machen, den Zugang für Bürger eröffnen und dabei den gesetzlichen Rahmen einhalten. Die Ursprünge der genutzten Programme liegen häufig noch in Großrechen-systemen der 70er Jahre bzw. Einzelplatzlösungen der 80er Jahre des letzten Jahrhunderts. Die mit den 90er Jahren beginnende sukzessive systematische Vernetzung der Systeme und deren Öffnung für öffentliche Netze resultiert in einer weltumspannenden Konnektivität. Die Komplexität des Gesamtsystems sowie seiner einzelnen Komponenten haben dabei massiv zugenommen. Reichte es in den 80er Jahren noch aus, das Büro abzusperren, sind seither die Anforderungen an IT-Sicherheit extrem gestiegen. Dem Schutzbedarf der verarbeiteten Daten kommt dadurch ein immer größerer Stellenwert zu.

Daher müssen bei der (Neu-)Auswahl von Anwendungen besondere Kriterien an die Sicherheit der Programme gestellt werden. Ebenso empfiehlt es sich, bestehende Verfahren auf die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit des Programms und der Daten zu überprüfen.

Hieraus können konkrete Maßnahmen für die einzelnen Anwendungen abgeleitet werden.

PRÜFUNG EINGESETZTER TECHNOLGIEN

Ein Großteil der Anwendungen basiert auf verbreiteten (Grundlagen-)Technologien von Drittanbietern. Hierbei kann es sich um Laufzeitumgebungen (Runtimes, beispielsweise Java) oder auch Module (Plug-Ins, zum Beispiel bei der PDF-Aufbereitung) handeln. Die Bereitstellung von Hotfixes, Patches und Updates für diese Programmteile liegt somit außerhalb der direkten vertraglichen Beziehung der Gemeinde zum Fachanwendungshersteller.
Es muss daher sichergestellt werden, dass

- für Sicherheitsprobleme der zugrundeliegenden Techniken schnellstmöglich Programmaktualisierungen (Hotfixes, Patches Updates) bereitgestellt werden und
- diese zeitnah durch den Anwendungshersteller zur Installation freigegeben werden.

So kann das Sicherheitsniveau bei besonders schützenswerten Daten (beispielsweise personenbezogenen Daten, Sozialdaten, Steuerdaten, …) auf dem höchstmöglichen Niveau gehalten werden.

§ Bereits beim Kauf- und Pflegevertrag (EVB-IT) müssen konkrete Regelungen zu Hotfixes, Patches und Updates (auch von Drittanbietersoftware) getroffen werden.

Stand der Technik ist die Realisierung von Anwendungen in 3-Tier-Architektur. Hierbei wird die Darstellung auf dem PC von der Verarbeitung auf dem Applikationsserver und der Datenspeicherung auf dem Datenbanksystem getrennt. Die zugrundeliegende Datenbank wird so von dem Client-PC und dem Anwender isoliert. Daraus ergibt sich, dass vom Client kein direkter Zugriff auf die Datenbank möglich ist. So wird vermieden, dass vom Client-PC außerhalb der Fachanwendung eine Änderung der Daten möglich ist. Dies gewährleistet die **Integrität** der Daten.
Die Kommunikation zwischen Client, Applikationsserver und Datenbankmanagementsystem sollte jeweils verschlüsselt erfolgen. Hierdurch wird die **Vertraulichkeit** erreicht.

Sofern Kommunikationsverbindungen nach außen bestehen (z. B. zu einem Dienstleister oder einem behördlichen Register), ist sicherzustellen, dass die Daten und der Übermittlungsweg verschlüsselt (und ggf. signiert) werden, um die **Vertraulichkeit** (und **Integrität**) sicherzustellen.

Sowohl die Client-Anwendung wie auch die Komponenten des Applikations-servers müssen gegen irreguläre Datenzugriffe und -manipulationen gehärtet werden (Bspw. Injections - **Cross-Site-Scripting (XSS)** = Einschleusen von manipulierten Datenbankabfragen z. B. in Suchfelder). Dies gilt vor allem für Webanwendungen und -portale mit Zugriff auf Datenbanken.

- Das Webbackend muss Eingaben auf Code überprüfen und die Ausführung von HTML-Code, SQL-Statements und Scripting-Befehlen verhindern. Mit der Verwendung des HTML-Tag <b> im Eingabefeld einer Suchanfrage kann einfach getestet werden, ob HTML-Code angenommen wird.

In Kombination mit einer verschlüsselten Speicherung in der Datenbank kann so die **Vertraulichkeit** und **Integrität** bewahrt werden.

- Alle auf der Datenbank vorgenommenen Manipulationen (Neuanlegen, Änderungen, Löschen) von Datensätzen müssen in speziellen Log-Dateien des Fachverfahrens aufgezeichnet werden. So lassen sich vorgenommene Änderungen nachvollziehen. Die datenbankseitigen Protokolldateien sind nicht ausreichend. Der Zugriff auf diese Log-Dateien ist auf den Fachanwendungs-betreuer in der IT-Abteilung zu beschränken. Es handelt sich hierbei um eine Maßnahme zur Sicherstellung der **Vertraulichkeit** (Kontrollmöglichkeit der Suchanfragen) sowie **Integrität** (Kontrollmöglichkeit der Änderungen sowie Löschvorgänge).

- Bei einer Auswertung der Protokolldateien könnte es sich um eine Arbeitskontroll-maßnahme handeln. Vorab ist dies daher mindestens mit der Personalvertretung abzustimmen.

- Es wird empfohlen Ermächtigungen zur Einsichtnahme von Protokolldateien durch den IT-Bereich im Störungsfall bzw. bei Sicherheitsvorfällen organisatorisch abzuklären und diese schriftlich zu fixieren.

REDUNDANZ SCHAFFEN

Wichtige zentrale Anwendungen sollten redundant betrieben werden. Hierdurch ergibt sich eine höhere **Verfügbarkeit** der Anwendung.

VERWALTUNG VON BERECHTIGUNGEN

Generell muss bei den Benutzerberechtigungen das Minimalprinzip angewendet werden. Verkürzt dargestellt gilt: So wenige Rechte wie möglich, so viele Rechte wie nötig. Administratoren- oder Superuser-Accounts sollte ausschließlich für administrative Zwecke genutzt werden.

Auch bei Fachverfahren sollten Passwortrichtlinien berücksichtigt werden. Ein Rücksetzen des Passworts sollte ausschließlich durch den Fachanwendungs-administrator möglich sein.

Jedwede Zugriffe sollten immer durch ein Benutzer-/Rollen-System geregelt werden. Benutzern werden Rollen zugewiesen und diesen wiederum Berechtigungen. Das Benutzer-/Rollen-Konzept sollte dokumentiert sein und fortgeschrieben werden, so dass der Soll- und Ist-Zustand jederzeit verglichen werden kann.

DATENBANKZUGÄNGE

Auch Zugänge zu den Datenbanken innerhalb einer Fachanwendung müssen mit minimalen Rechten erfolgen. Oftmals erfolgen bei Fachanwendungen im Hintergrund Datenbankzugriffe mit generischen technischen Benutzerkonten und administrativen Rechten. Diese Benutzerkonten dürfen keinesfalls hartkodiert sein und die Kennwörter müssen individuell abänderbar sein. Passwörter dürfen nicht im Klartext abgespeichert werden. Darüber hinaus sind Initial-/Standardkennwörter unbedingt zu ändern.

DOKUMENTATION DES KONKRETEN SCHUTZBEDARFS

Bei der Feststellung und Dokumentation des konkreten Schutzbedarfs muss beachtet werden, dass Komponenten unterhalb der Anwendung (also z. B. (virtuelle) Server, Netzwerkkomponenten, etc.) automatisch als Schutzbedarf die höchste Klasse der Anwendungen erben, die die Komponente nutzen.

KONTAKT

Beispiele typischer Anwendungen im kommunalen Umfeld und Vorschläge zu deren Schutzbedarf sind auf der Behördennetz-Homepage des LSI unter https://www.lsi.bybn.de zu finden.
Kommunen ohne Zugang zum Behördennetz können die Datei per E-Mail anfordern. Bitte wenden Sie sich hier an Beratung-Kommunen@lsi.bayern.de.