Richtlinie zum Umgang mit dem System für Mandantenadministratoren

1 Vorbemerkungen

Dieses Diensteangebot richtet sich primär an Privatpersonen und an Kunden mit einer überschaubaren Anwendung. Daher ist davon auszugehen, dass der Kunde alle weiteren Nutzer persönlich kennt und ihnen hinsichtlich des Umgangs mit den Daten vertraut. Trotzdem sind nachfolgende Vorgaben zu beachten.

Beim Einrichten des Mandanten wird je ein Mandantenadministrator für den Kunden eingerichtet und dem Kunden werden die Zugangsdaten für seinen Mandantenadministrator mitgeteilt. Die Einrichtung weiterer User und das Anlegen von API-Keys obliegt dem Kunden, wobei nachfolgende Erläuterungen und Vorgaben zu beachten sind.

Um ein hohes Maß an Datensicherheit zu erzielen, wurden bei der Einrichtung des Mandanten geeignete Einstellungen vorgenommen. Diese Datensicherheit kann nur dann auf Dauer gewährleistet werden, wenn die Mandantenadministratoren bei ihrer Tätigkeit folgende Richtlinien befolgen.

2 Rollen- und Berechtigungskonzept

Das System ELEMENT lässt sehr flexibel die Vergabe von Berechtigungen zu. Das kann allerdings auch dazu führen, dass unbeabsichtigt Berechtigungen erteilt werden, die missbräuchlich genutzt werden können.

Benutzern und API-Keys ist zunächst eine Rolle zuzuweisen, wobei

- Read-only / Lesend
- User / Benutzer
- Admin / Administrator

zur Auswahl stehen. Bei „Lesend“ stehen nur Leserechte zur Verfügung. Für „Benutzer“ werden weitergehend Berechtigungsprofile in sog. Gruppen festgelegt. Hier kann in verschiedenen Kategorien festgelegt werden, ob Elemente gelesen, erstellt und/oder bearbeitet werden dürfen. Mandantenadministratoren haben sehr weitgehende Berechtigungen; diese Rolle sollte nur Anwendern mit speziellen Aufgaben im Bereich der Administration des Mandanten, wie z. B. Anlegen oder Sperren von Benutzern, zugewiesen werden.

In der Grundeinstellung des Systems sind 3 Gruppen vordefiniert, um den Mandantenadministratoren die Arbeit zu vereinfachen:

- Lesend: Lesezugriff auf Geräte und Ordner sowie Streams, Regeln, Profile und Ansichten
- Anwender: ausreichend für Nutzer, die typische Arbeiten mit Geräten ausführen müssen; umfasst weitergehende Rechte für Geräte und Ordner inklusive Anlegen

und Bearbeiten sowie Leserechte für Streams, Regeln, Profile, Ansichten, Gerätevorlagen, Parser und Hintergrundjobs
- Entwickler: umfasst sämtliche Berechtigungen in allen Kategorien mit Ausnahme von User und API-Keys

Nach Möglichkeit sollte ausschließlich mit den vorgegebenen Rollen und den vordefinierten Gruppen gearbeitet werden. Zusätzliche Gruppen sollten nur definiert werden, wenn Anwender keiner Rolle oder Gruppe aus dem vorgegebenen Vorrat sinnvoll zugeordnet werden können. Dabei ist insbesondere zu beachten, dass keine Berechtigungen aus den Kategorien „BENUTZER" und „APIKEYS" vergeben werden. Diese Berechtigungen sollten den Mandantenadministratoren vorbehalten bleiben, da durch ihre Nutzung bewusst oder unbewusst Zugriffsmöglichkeiten für weitere Personen oder Systeme geschaffen werden können.

Grundsätzlich sollte bei der Vergabe von Berechtigungen nach dem Minimalprinzip vorgegangen werden, d.h. es sollte für Benutzer und API-Keys nur die Rolle/Gruppe ausgewählt werden, die für den Anwendungsfall tatsächlich benötigt wird.

3 API-Keys

API-Keys dienen dem Systemzugriff von anderen Systemen aus, um z. B. Daten zur Weiterverarbeitung abzurufen. Das Rollen- und Berechtigungskonzept entspricht demjenigen für Benutzer.

Im Hinblick auf den Datenschutz ist es wichtig nachvollziehen zu können, wer bestimmte Aktionen ausgeführt hat. In ELEMENT sind API-Keys systemtechnisch nicht personenbezogen, so dass eine über einen API-Key ausgeführte Aktion systemtechnisch nicht auf eine Person zurückgeführt werden kann. Um diese Möglichkeit auf anderem Wege zu schaffen, muss für API-Keys auf organisatorischem Wege ein Personenbezug hergestellt werden. Dazu ist sicherzustellen, dass API-Keys ausschließlich von Mandantenadministratoren angelegt werden können (siehe 2 Rollen- und Berechtigungskonzept) und Mandantenadministratoren beim Anlegen wie folgt verfahren:

- Ein neuer API-Key wird immer für einen bestimmten Benutzer angelegt; falls mehrere Benutzer API-Keys mit denselben Berechtigungen benötigen, ist eine entsprechende Anzahl von API-Keys zu erzeugen.

- Der erzeugte API-Key ist auf sicherem Weg (z.B. verschlüsselte E-Mail) ausschließlich demjenigen Benutzer mitzuteilen, für den er angelegt wurde.

Zur Vermeidung von Problemen bei datenschutzrechtlichen Vorfällen ist die Einhaltung dieser Vorgaben zwingend erforderlich.

Als zusätzliche Maßnahmen zur Erhöhung der Sicherheit empfiehlt es sich grundsätzlich, die Gültigkeit von API-Keys zu begrenzen (nach Anlegen eines API-Keys in den Eigenschaften möglich), sowie API-Keys turnusmäßig zu erneuern (z.B. einmal jährlich).

4 E-Mail-Benachrichtigungen

Zur Einschränkung des E-Mail-Empfängerkreises und zum Schutz vor Missbrauch (z.B. Spam-Versand) müssen Empfänger-Domains in die E-Mail-Whitelist (unter „Einstellungen / Allgemein“) eingetragen werden – Schema: @beispiel1.de,@beispiel2.de
Die Whitelist-Einträge dürfen sich nur auf notwendige Domains beschränken.

5 Weitergabe dieser Richtlinie

Diese Richtlinie ist für die Verantwortlichen beim Auftraggeber sowie für die Mandantenadministratoren für den verantwortungsvollen und Sicherheit gewährleistenden Umgang mit den Administrationsmöglichkeiten gedacht und darf nicht an andere Personen weitergegeben werden.

Beim Anlegen eines weiteren Mandantenadministrators ist diese Richtlinie mit der Bereitstellung der Zugangsdaten weiterzugeben.