

Bericht

2. Workshop

„Zugang zu Verwaltungsleistungen für Unternehmen über Unternehmenskonten“ - Schwerpunkt: Rechte und Rollen

Bundesministerium für Wirtschaft und Energie, Berlin

07. August 2019

**Koordinierungsprojekt „Unternehmenskonto/-en“ des IT-Planungsrates
unter Federführung der Freien und Hansestadt Bremen**



Im Rahmen des Koordinierungsprojektes „Unternehmenskonto/-en“ des IT-Planungsrates wurde am 16./17. Mai 2019 ein erster Workshop mit Vertretern aus Wirtschaftsverbänden und Unternehmen in Bremen durchgeführt. Ziel war es, den Austausch mit der Wirtschaft anzustoßen und deren Bedürfnisse und Anforderungen an Unternehmenskonten zu erheben. Es wurden allgemeine Erwartungen der Unternehmen und Verbände an die Umsetzung des Onlinezugangsgesetzes (OZG) erhoben sowie diverse Anforderungsbündel an ein Unternehmenskonto¹ der Verwaltung identifiziert, das flächendeckend in Deutschland zur Verfügung gestellt werden soll. Ein zentrales Ergebnis des Workshops war die Erkenntnis, dass weitere Digitalisierungslabore bzw. Workshops wünschenswert sind, um die u.a. nach Unternehmensgröße und -branche unterschiedlichen Anforderungen an das Unternehmenskonto zu erheben und ein tragfähiges Gesamtkonzept zu erarbeiten.

Insbesondere sollten das Anforderungsbündel „Rechte und Rollen“ und die spezifischen Anforderungen von Großunternehmen gezielt bearbeitet werden. Dies stand im Mittelpunkt des zweiten Workshops am 07. August 2019 im Bundesministerium für Wirtschaft und Energie, der in Zusammenarbeit des Landes Bremen und der Arbeitsgemeinschaft für wirtschaftliche Verwaltung (AWV) durchgeführt wurde.

Teilnehmer des Workshops waren Vertreter von Großunternehmen (wie Siemens, Volkswagen Financial Services, Techniker Krankenkasse, Haufe, Bearing Point, Schütze AG, T-Systems, Deutsche Telekom, Bremer Lagerhaus Gesellschaft), von Verbänden (wie DIHK, DGUV) von Bundesministerien bzw. -behörden (wie Bundesnetzagentur, BAFA, BMVI, BMWi) und Mitgliedern der Koordinierungsgruppe „Unternehmenskonto/-en“.



¹ Aus Gründen der Lesbarkeit wird im Folgenden der Singular verwendet, da unter allen Teilnehmenden Konsens herrschte, dass ein Unternehmen künftig nur ein einziges Unternehmenskonto benötigt, mit dem alle digitalen Services der Verwaltung genutzt werden können.

In den drei Gruppen wurde anhand je einer Verwaltungsleistung (Mutterschutzmeldung, Kfz-Anmeldung, Genehmigung eines Schwerlasttransportes) der Soll-Prozess im Unternehmenskonto betrachtet und die Rollen und Rechte erarbeitet, um diesen Prozess abzuwickeln. Im Brainstorming wurden in den drei Gruppen anhand verschiedener Anwendungsfälle (u.a. Vertretungsregelungen, Vollmachtserteilung an externe Dienstleister, Unternehmensverflechtungen in Konzernstrukturen) die Anforderungen an die Rechte- und Rollen-Administration im Unternehmenskonto zusammengetragen und diskutiert.

Grundsätzliche Anforderungen an Berechtigungs- und Rollenverwaltung

- Die Berechtigungs- und Rollenverwaltung muss in der Verantwortung und Hoheit der Unternehmen liegen. Das Unternehmenskonto muss die technischen Möglichkeiten bieten, dass Unternehmen die Rollen und deren Rechte gemäß ihrer internen Strukturen einrichten können.
- Die Konfiguration sollte eine gute, intuitive Bedienbarkeit für Unternehmen gewährleisten und den damit verbundenen Aufwand für die Unternehmen gering halten.
- Für die Übernahme von vorhandenen Berechtigungskonzepten bzw. -systemen im Unternehmen (z.B. aus einem ERP-System) sollten Schnittstellen geschaffen werden. Es wird daher auch empfohlen, Anbieter von ERP-Systemen oder Active Directory in die Umsetzungskonzeption des Unternehmenskontos einzubinden.
- Es wird empfohlen, für die Authentisierung Open ID Connect zu unterstützen.
- Die große Mehrheit der Verwaltungsleistungen sollte über Machine-2-Machine-Kommunikation automatisiert abgewickelt werden können, vor allem bei Großunternehmen. Es soll geprüft werden, wie das Unternehmenskonto M2M-Kommunikation unterstützen kann und Schnittstellen dazu bereitstellen bzw. vorhandene Standardschnittstellen bedienen kann. Ein mögliches Beispiel ist die intelligente Ablage von Massenbescheiden im Postfach.
- Rollen im Unternehmenskonto müssen einheitlich für Web-Login und M2M-Kommunikation administriert werden können.
- Die Verwaltungsapplikation (also das Portal bzw. der Online-Dienst) muss die Berechtigung der Rolle prüfen. (Jemand, dem das Unternehmen im Unternehmenskonto nur die Rolle und Berechtigung für die Zulassung von Kfz zugewiesen hat, darf in einem Online-Service keine Umsatzsteuervoranmeldung einreichen oder auf entsprechende Bescheide zugreifen dürfen.)

Abbildung von Unternehmens- und Konzernstrukturen und Beziehungen zwischen mehreren Unternehmen

- Für jedes Unternehmen im Sinne einer eigenen Rechtseinheit muss es ein eigenes Unternehmenskonto geben. Allerdings muss vorher einheitlich und klar definiert werden, was „ein Unternehmen“ in diesem Sinne ist.
- Mehrfache Registrierungen von Unternehmenskonten für ein Unternehmen sollten ausgeschlossen werden. Für eine eindeutige Zuordnung wäre die Realisierung eines zentralen Unternehmensregisters wichtig.
- Konzernstrukturen und Aufbauorganisationen unterscheiden sich stark zwischen verschiedenen Unternehmen und sind bei Großunternehmen komplexer. In dem Unternehmenskonto bzw. in den Unternehmenskonten müssen daher Unternehmen die Berechtigungen so konfigurieren können, dass ihre Konzernstrukturen und Hierarchien abbildbar sind.
- Das betrifft auch die Beziehungen zwischen verschiedenen Unternehmen (Rechtseinheiten) eines Konzerns. Diese sollen durch die Verknüpfung von Unternehmenskonten oder die Vererbbarkeit von Vollmachten abgebildet werden können. So übernehmen beispielsweise einzelne Mutter- oder Tochterunternehmen eines Konzerns (z.B. als Shared Service Center) Verwaltungsleistungen für andere Tochterunternehmen im Konzern. Ähnliches gilt für Intermediäre. Die Vertretungsbefugnis dieser Unternehmen und ihrer Mitarbeiter muss im Unternehmenskonto abgebildet werden können. Die Berechtigungen müssen von Unternehmen zu Unternehmen übertragbar sein.
- Unternehmen müssen von ihnen bevollmächtigte Intermediäre nachvollziehbar festlegen und berechtigen können.

Rollen und Rechte

- Folgende Rollen und Rechte erscheinen sinnvoll: Super-Administrator (Prokurist, Geschäftsführer), Gruppen-Administrator (z.B. für Abteilung), (diverse) Sub-Administratoren, Antragsberechtigte (Mitarbeiter)
 - Super-Administrator (mit Prokura): Unternehmenskonto registrieren, löschen, Unternehmensdaten im Konto eintragen/ändern, Administratoren einrichten und autorisieren
 - (Sub- oder) Gruppen-Administrator: Nutzer löschen, deaktivieren, einrichten, Funktionsrollen einrichten und für Verwaltungsleistung autorisieren, Nutzer Funktionsrollen zuweisen, Gruppen-Funktionsrollen zuweisen.
 - Der Sub-Administrator kann für bestimmte Themengebiete Rollen delegieren. Der Rolleninhaber kann eine ihm zugewiesene Rolle nicht ohne Zustimmung des Sub-Administrators delegieren.
 - Nutzer/Antragsteller: Anträge bearbeiten (für zugewiesene Verwaltungsleistung), Anträge (nur) lesen, bearbeiten, abschicken; Postfach (für zugewiesene Verwaltungsleistung) lesen, beantworten
- Ein nicht zugewiesenes Recht bedeutet kein Recht.

- Es sollte zudem die Möglichkeit bestehen, auch unterschiedliche Berechtigungen für eine Leistung verteilen zu können (z.B. Antrag stellen, einsehen, Bescheid einsehen).
- Vertretungsregelungen obliegen dem Unternehmen.
- Im Unternehmenskonto wird den Rollen angezeigt, für welche Verfahren oder Bündel von Verfahren eine Berechtigung vorliegt. Nur gegenüber diesen Leistungen können sie sich mit dem Konto authentifizieren.

Konfigurationsmöglichkeiten

- Hinsichtlich der Berechtigungen haben Unternehmen unterschiedliche Anforderungen. Deshalb muss das Berechtigungskonzept des Unternehmenskonto für Unternehmen frei konfigurierbar sein (gruppenabhängig, personenabhängig, ortsabhängig).
- Die Rollen sollten kaskadierend eingerichtet werden können. Die Anzahl der Kaskaden, die dazugehörigen Rollen und Rechte müssen frei wählbar sein. Das Unternehmenskonto sollte aber vordefinierte Leistungsgruppen (z.B. Personal, Steuern) anbieten.
- Für das Postfach bzw. den Rückkanal von der Verwaltung zum Unternehmen müssen die Berechtigungen von der Antragstellung gespiegelt werden. Zugleich müssen die Rechte und Rollen beim Rückkanal frei konfigurierbar und Berechtigungen ggf. anders verteilt werden können. Unternehmen sollten dafür Rückkanal-Adressen für Verwaltungsleistungen hinterlegen können (z.B. Funktionspostfächer).
- Im Unternehmenskonto soll hinterlegt werden können, welcher Kommunikationskanal als Rückkanal benutzt werden soll, beispielsweise das Postfach im Unternehmenskonto (mit Benachrichtigung über Eingang im Unternehmenskonto), E-Mail, M2M-Nachricht.
- Auch das Postfach sollte so konfigurierbar sein, dass beispielsweise Funktions- bzw. Bereichspostfächer eingerichtet werden können.
- Die Leistungen der Verwaltung sollten als Grundlage für das Rollenkonzept dienen. Die Administration des Rollenmodells sollte auf der Ebene der OZG-Leistungen (nicht der kleinteiligeren LeiKa-Leistungen) erfolgen. Die OZG-Leistungen sollten überordnet geclustert werden können (z.B. Personal, Steuern), um entweder von einer Person wahrgenommen zu werden (z.B. KMU) oder als Sub-Admin weiterdelegiert zu werden. Der Aufwand für Unternehmen sollte hier so gering wie möglich gehalten werden.
- Die Einrichtung eines Unternehmenskontos sollte durch die Bereitstellung von Blue Prints (für typische Geschäftsvorfälle) bzw. von Musterkonten für verschiedene Unternehmensgrößen und -branchen unterstützt werden. Muster-Rollen werden vordefiniert, die dann vom einzelnen Unternehmen leichter angepasst werden können.
- Im Unternehmenskonto sollen keine Workflows abgebildet werden. Für die Erteilung von Berechtigungen müsste jedoch ein 4-Augen-Prinzip umsetzbar sein.

Weitere Anforderungen an Unternehmenskonto

- Die Einführung und das Roll-out des Unternehmenskontos müssen sehr gut vorbereitet werden. Kommunikations- und Trainingsmaßnahmen sollten gut geplant werden.

Anforderungen an Online-Services

- Die Dokumentation von Datentransfers (insbesondere von mitarbeiterbezogenen Daten) muss gewährleistet sein. Bei einem Datentransfer an die Verwaltung muss eine Empfangsbestätigung im Postfach gespeichert werden können.
- Stammdaten und rollenspezifische Antragsdaten sollen wiederverwendbar sein (nicht im Unternehmenskonto, sondern in Antragsverfahren). Dabei ist zu prüfen, ob diese Daten im Unternehmenskonto aufbewahrt werden können oder in der Antragsmanagement-Plattform.

Diskussion

Im Rahmen der Diskussion wurde von den Unternehmensvertretern erneut bekräftigt, dass alle Verwaltungsleistungen mit einem einzigen Unternehmenskonto nutzbar sein müssen. Mit Blick auf die Möglichkeit, verschiedene Lösungen interoperabel zu gestalten, wurde erhebliche Skepsis geäußert, dass dies bewältigt werden kann. Mit Verweis auf Initiativen wie Verimi wurde unterstrichen, dass im Rahmen der Digitalisierung neue Wege der Kooperation und Zusammenarbeit gegangen werden müssen. So haben sich mehrere große deutsche Unternehmen branchenübergreifend zusammengetan, um eine gemeinsame Identitätsplattform zu entwickeln (u.a. Volkswagen, Lufthansa, Deutsche Bank, Deutsche Telekom, Allianz) und dabei den Investitionsschutz und Partikularinteressen nach hinten gestellt. Deshalb sei die Erwartung der Unternehmen, dass auch die Verwaltung bereit sein müsse, sich den Anforderungen der digitalen Transformation zu stellen und sich von bestehenden Strukturen zu lösen. Teilnehmer wiesen darauf hin, dass eine Umsetzung des Unternehmenskontos, die die Unternehmensrealität nicht hinreichend widerspiegelt und deshalb nur mit hohem Aufwand einzuführen und zu nutzen sei, zur Folge hätte, dass das Unternehmenskonto nur wenig genutzt werde.

Ausblick

Die Koordinierungsgruppe Unternehmenskonto stellte den weiteren Fahrplan für die Diskussion der Anforderungen und Umsetzung vor. So würden die Ergebnisse in der nächsten Sitzung der Projektgruppe eID Ende August behandelt. Im September seien zwei Sitzungen mit den IT-Dienstleistern der Länder und möglichen weiteren IT-Dienstleistern geplant, eine bei der Föderalen IT-Kooperation (FITKO) und eine mit der Koordinierungsgruppe. Teilnehmer sprachen sich dafür aus, auch Dienstleister aus der Privatwirtschaft, z. B. Verimi oder Anbieter von ERP- oder IAM-Systemen miteinbeziehen. Die Koordinierungsgruppe berichtete, dass dieser Workshop und die angekündigten Sitzungen dazu dienen, einen Beschluss zum Unternehmenskonto bei der nächsten Sitzung des IT-Planungsrates am 24. Oktober vorzubereiten.