Zugriffe auf Daten, Systeme Prozesse

Regelungen (aus dem Baustein 51 SDM)[1]

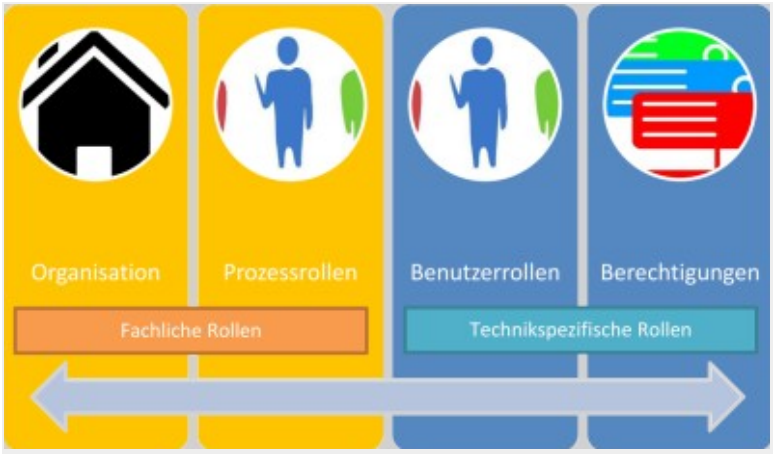
Der Umfang einer Dokumentation hängt sicherlich von der Anzahl der verschiedenen Verarbeitungstätigkeiten (Prozesse) und der dafür notwendigen Beteiligten (Mitarbeiter) ab.

1. Hinweise

(a) Bereich technisch – organisatorische Maßnahmen (TOM)

„Für alle möglichen Datenzugriffe müssen die Gewährleistungsziele mit Blick auf die Rollen bzw. Personengruppen sowie auf die Systeme und Dienste erfüllt werden. Dies bedeutet insbesondere, dass nur solche Zuständigkeiten und Berechtigungen vergeben werden dürfen, welche für die Ausführung der jeweils erforderlichen Verarbeitungsschritte notwendig sind.“ (Zitat: Seite 2 Baustein 51 des SDM)

Im Verfahrensverzeichnis ist die Erhebung und Verarbeitung u. a. beschrieben. Im Konzept für die Rollen und Berechtigungen sind die (notwendigen) fachlichen und technischen Rollen festzulegen.



Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“ Seite 4;
Abb. 2: Zusammenhang zwischen fachlichen und technik - spezifischen Rollen

i) Fachliche Rollen

Wer darf was in der Verarbeitung vornehmen und braucht dazu welche, notwendigen Zugriffe.

ii) Technische Rollen

Wer ist für (die Sicherheit) welcher Anwendung verantwortlich und vergibt die Zugriffsberechtigungen.

„Bei dieser Verbindung hat der Verantwortliche zu gewährleisten, dass alle fachlichen Anforderungen an die Verarbeitungstätigkeit vollständig in die technische Ebene transformiert werden. Der Verantwortliche MUSS aus struktureller und funktionaler Sicht spezifizieren, wie die jeweiligen Verarbeitungstätigkeiten und die davon umfassten Aktivitäten mit der Unterstützung von eingesetzten Systemen und Diensten realisiert werden.“ (Zitat: Seite 4 Baustein 51 des SDM)

(b) Bereits vorhanden?

Im ***Verfahrensverzeichnis*** sind i. d. R. die Verarbeitungstätigkeiten und die damit verbundenen Anwendungen aufgeführt (fachliche Rollen). Dazu hilfreich ist die (eine) ***digitale Inventur*** mit Hardware, Software, Plattformen, digitale Präsenz & Service, den Verantwortlichen und Zugriffsberechtigten (technische Rollen). Aus einem Abgleich der beiden Verzeichnisse sind die jeweiligen Rollen (nach Mitarbeiter, Anwendungen, Einheiten), sofern nicht bereits erfolgt, recht einfach abzuleiten und festzulegen. Einmal dokumentiert lassen sich bereits frühzeitig in der Planungsphase von Änderungen oder Neuerungen diese erkennen und ändern bzw. aufnehmen – nicht nur in der Dokumentation.

(PS: Natürlich ist auch bei den Berechtigungen zu unterscheiden nach Lesen – Schreiben – Löschen - Transfer)

2. Richtlinie für ein Berechtigungskonzept

Je nach der Größe der Organisation ist zur verständlichen Information der Mitarbeiter eine übersichtliche Richtlinie hilfreich

Nachfolgenden Entwurf bitte jeweils aktuell und individuell prüfen und anpassen (Stand: 11/2021)[2]

1 *Quelle: Standard Datenschutz Modell - Baustein 51: (PDF) „Zugriffe auf Daten, Systeme und Prozesse regeln“*
2 *Basisvorlage: DATENSCHUTZ-GRURU: „Richtlinie für das Berechtigungsmanagement“*

Richtlinie zum Berechtigungskonzept der Organisation/Unternehmen

1. Präambel

In unserer Organisation kommen diverse IT – Ressourcen (Hardware, Software, Systeme, Cloud, Plattformen u. a.) zum Einsatz. Bei der Einrichtung und Änderung von diesen IT-Ressourcen ist zu gewährleisten, dass die Anforderungen an die Informationssicherheit und die datenschutzrechtliche Vorgaben eingehalten werden. Dies soll auch durch die verbindlichen Vorgaben in dieser Richtlinie zum Management des Berechtigungskonzeptes umgesetzt werden. Die Vorgaben dieser Richtlinie sind an das IT – Grundschutz - Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI) – insbesondere den Baustein ORP.4 Identitäts- und Berechtigungsmanagement – angelehnt.

2. Geltungsbereich

Diese Richtlinie gilt für alle Standorte. Sie verpflichtet alle Beschäftigten der Organisation/Unternehmen zur Einhaltung der hier festgelegten Vorgaben.

3. Vorgaben für das Berechtigungskonzept

(a) Grundsätzliche Vorgaben zum Management von Berechtigungen

Vor jeder Inbetriebnahme einer IT - Ressource ist eine **„verantwortliche Person“** und eine oder mehrere **„administrierende Person(en)“** für die IT – Ressource (IT - System oder die Anwendung) zu bestimmen.

Die **verantwortliche Person** bestimmt in Abstimmung mit den administrierenden Personen, ob und in welchem Umfang von wem auf die IT-Ressource zugriffen werden kann.

In diesem Zusammenhang sind Berechtigungen für verschiedene Arten von Anwendern/innen in „Benutzerrollen/-gruppen“ zusammenzufassen, um einzelnen Anwendern/innen bei der Einrichtung eines Zugangs die passende Rolle zuweisen zu können.

(b) Regeln für die Einrichtung von Berechtigten

Für jede IT-Ressource muss eine separate administrative Rolle eingerichtet werden, die den administrierenden Personen für die IT-Ressource zugeordnet wird.

Neue Benutzergruppen dürfen ausschließlich von administrierenden Personen unter Einbeziehung der jeweiligen verantwortlichen Person für die IT-Ressource eingerichtet werden. Bei der Einrichtung von Benutzergruppen ist der Grundsatz der Erforderlichkeit und des tatsächlichen Bedarfs zu berücksichtigen.

Neue Anwender/innen dürfen nur nach dem „Vier-Augen-Prinzip“ eingerichtet werden. Die Einrichtung eines Anwenders/in erfolgt durch eine administrierende Person der jeweiligen IT-Ressource, wenn die nachfolgenden Voraussetzungen vorliegen:

(1) Die Einrichtung einer Berechtigung wird von der verantwortlichen Person für die IT-Ressource unter Angabe des Namens und ggf. weiterer Kontaktdaten bei einer Administrator/in in Textform (z.B. über ein Ticket-System) angefordert.

(2) Die verantwortliche Person teilt der jeweils administrierenden Person die Benutzergruppe für die Zuordnung des neuen Anwenders/in mit.

(3) Die verantwortliche Person wird beim Antrag das Prinzip der Notwendigkeit beachten. Danach sind Anwendern/innen nur die Rechte zuzuweisen, die für die zugewiesenen Aufgaben im Unternehmen tatsächlich erforderlich sind.

(4) Wenn ein Anwender/in über die Rechte der zugeordneten Benutzergruppe hinaus mehr Rechte erhalten soll, sind diese von der verantwortlichen Person bei den administrierenden

Personen zu definieren und zu begründen. Gleiches gilt für ein „Weniger“ an Berechtigungen.

Die administrierende Person wird sich bei Unklarheiten über Art und Umfang der Berechtigungen für einen Anwender/in mit der verantwortlichen Person in Verbindung setzen.

(c) Dokumentation von Benutzergruppen und deren Berechtigungen

Die administrierende Person einer IT-Ressource ist verpflichtet, die Einrichtung, Änderung und den Entzug von Berechtigungen zu dokumentieren. Gleiches gilt für Benutzergruppen. Die Dokumentation ist vor unberechtigtem Zugriff zu schützen. Die Verfügbarkeit und die Integrität der Dokumentation sind zu gewährleisten.

(d) Regelung für die Änderung und den Entzug von Berechtigungen

Bei personellen Veränderungen von Anwendern/innen sind die Berechtigungen von den administrierenden Personen anzupassen. Die verantwortliche Person ist verpflichtet, die administrierenden Personen über personelle Veränderungen zu informieren, wenn diese Auswirkung auf den tatsächlichen Bedarf von Berechtigungen für Anwender/innen haben können. Eine Information muss insbesondere erfolgen, wenn Anwender/innen das Unternehmen verlassen.

(e) Regelung des Passwortgebrauchs

Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 12 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.

Ein Passwortwechsel ist grundsätzlich nicht oder regelmäßig nach X Tagen vorgesehen. In begründeten Ausnahmefällen, z. B. bei Verdachtsmomenten ist eine kurzfristige Erneuerung des Passwortes möglich. Eine Passworthistorie ist hinterlegt. So wird sichergestellt, dass die vergangenen zehn Passwörter nicht noch einmal verwendet werden können.

Fehlerhafte Anmeldeversuche werden protokolliert. Bei 3-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Zugangs des Anwenders/in.

Die administrierenden Personen einer IT-Ressource sind verpflichtet, beim Zurücksetzen von Passwörtern sichere Verfahren zur Vergabe von neuen Passwörtern für Anwender/innen einzusetzen. Ziel ist es, sicherzustellen, dass Unbefugte durch eine Passwortzurücksetzung keinen Zugriff auf IT-Ressourcen erhalten. Unberechtigte Zugriffsversuche auf IT-Ressourcen sind so zu beschränken, dass bei mehrfachen Zugriffen mit falschen Zugangsdaten eine (temporäre) Sperrung des jeweiligen Zugangs erfolgt.

4. Regelmäßige Aktualisierung („Monitoring“)

Jede verantwortliche Person ist verpflichtet, in regelmäßigen Abständen – mindestens jedoch einmal jährlich – zu überprüfen, ob die Berechtigungen der Anwender/innen aktuell noch dem Prinzip der Notwendigkeit entsprechen. Hierzu kann die verantwortliche Person eine aktuelle Übersicht der erteilten Berechtigungen für die IT-Ressource von der jeweils administrierenden Person verlangen.

Wenn ein Anwender/in Zugriffsrechte auf die IT-Ressource hat, die nicht für die zugewiesenen Aufgaben tatsächlich erforderlich sind, dann hat die verantwortliche Person die administrierende Person aufzufordern, die Rechte entsprechend anzupassen.

5. Sanktionen

Ein Verstoß gegen diese Richtlinie kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.