Wer darf was?

Die wasserdichte Prüfung von Berechtigungskonzepten

Der Zugriff auf Unternehmensdaten muss geschützt werden – dies ist sicherlich die Kernaussage jedes Unternehmens. Viele Administratoren klagen jedoch über undurchsichtige Konzepte und Ausnahmeregelungen bzw. haben schon komplett den Überblick verloren. Wie sind die Daten sinnvoll zu schützen, und wie prüfen Sie als DSB ein datenschutzkonformes Berechtigungskonzept?

„Ein Berechtigungskonzept beschreibt ein System, in dem die Nutzung von Ressourcen nicht uneingeschränkt möglich ist, sondern es erfolgt je Benutzer und Ressource eine genaue Definition der Nutzung“, soweit Wikipedia.

Doch wie eine sinnvolle und nachvollziehbare Umsetzung erfolgen kann, darüber schweigt auch Wikipedia.

Ein einheitliches System wäre die Ideallösung

Ideal wäre, auch im Sinne einer nachvollziehbaren Datenschutz-Prüfung, wenn es nur ein System und ein gut strukturiertes Berechtigungskonzept im Unternehmen geben würde. Das ist angesichts der unterschiedlichen IT-Strukturen leider noch Fiktion.

Vielfältige IT-Stukturen und ebenso vielfältige Arbeitsweisen

Jedes System erfordert eine eigene Betrachtungsweise. Zudem arbeiten die zuständigen Administratoren in ihrem Aufgabengebiet erfahrungsgemäß jeweils ein bisschen anders.

Ihr Prüfauftrag: Schwerpunkt auf die personenbezogenen Daten

Es ist nicht einfach, im Unternehmen das Berechtigungskonzept zu prüfen. Ihr eigentlicher Prüfauftrag liegt zudem schwerpunktmäßig darauf, zu verhindern, dass personenbezogene Daten von Unberechtigten gelesen oder manipuliert werden können.

Als DSB zwischen den Fronten

Kommen Sie mit Ihrer Prüfanfrage in die Fachabteilung, wird vermutlich erst einmal die Nase gerümpft. Mein Sicherheitskonzept ist in Ordnung – läuft schon über Jahre – noch keiner hat sich beschwert – was wollen Sie?

Klären Sie daher zunächst auf, weshalb Sie an dem Berechtigungssystem interessiert sind.

Prüfkonzept erstellen

Bevor Sie an die „Front“ gehen, ist es ratsam, sich mit dem zu prüfenden System vertraut zu machen. Als Beispiel sei die Kontrolle eines Entgeltabrechnungssystems vorgestellt.

Beispiel Rollenzuordnung

User	Rolle PayAll	Rolle PayPflege	Rolle PayBeweg
Wichtig Edith	X		
Lorz Franz		X	
Fänkli Judit		X	X

Kritische Fragen – auf was achten?

Erstellen Sie sich Notizen, um bei der Prüfung vor Ort nicht in Fettnäpfchen zu treten. Wenn Sie zu ahnungslos an eine Kontrolle herangehen, wird Ihnen nicht selten ein Flopp als ein Topp verkauft, soll heißen, der Admin wickelt Sie um den Finger.

Weisen Sie eine durchdachte Struktur bei den Kontrollfragen vor, haben Sie den Respekt Ihres Gesprächspartners schon halb gewonnen.

Ein gutes Berechtigungskonzept weist Nichtzugriffsberechtigte in die Schranken.

1. Prüfschritt: Benutzeraccount

Ein strukturiertes Berechtigungskonzept beginnt bei der Neudefinition eines Users. Ein Benutzerkonto, egal in welchem System, muss mit einem starken Kennwort ausgestattet sein.

Prüfen Sie also, ob folgende Einstellungen bei der Benutzerdefinition gesetzt wurden:

- Kennwortlänge (größer/gleich 6 Zeichen)
- automatisierte Kennwortalterung (weniger als 60 Tage)
- Aufbau des Passwortes (Groß-/Kleinschreibung, Sonderzeichen, Zahlen); keine Trivialpasswörter
- Sperre bereits verwendeter Passwörter

Das beste Berechtigungskonzept nützt dem Datenschutz nichts, wenn sich ein unberechtigter Nutzer mit einem Trivialkennwort oder einer allgemeinen unternehmensspezifischen Zugangs-

kennung als X-beliebiger Benutzer authentifizieren kann.

2. Prüfschritt: Erlauben Sie auf gar keinen Fall Gruppenuser

Nicht selten machen es sich die Verantwortlichen aus der IT einfach und definieren ein oder zwei Gruppenuser für die Anwendung. Die Mitarbeiter nehmen heute mal diesen und morgen jenen Benutzeraccount.

An eine nachvollziehbare „Eingabekontrolle" nach § 9 BDSG und Anlagen ist so nicht zu denken. Empfehlenswert daher: konsequent verbieten und auf einer namensbezogenen Authentifizierung bestehen!

3. Prüfschritt: Funktionsrollen

Idealerweise werden Berechtigungen in Form von Funktionsrollen vergeben. Eine Rollenberechtigung ist wesentlich leichter zu handhaben, v.a. bei Änderung der Aufgaben eines Benutzers. Im Fall der Entgeltabrechnung würden u.a. folgende Prüfschritte anfallen:

- dedizierte Zugriffsvergabe bei Mehrmandantensystemen bzw. Abrechnungskreisen
- Rollendefinition mit Rollenbeschreibung und entsprechenden Zugriffsregelungen prüfen
- Berechtigung zur Stammdatenänderung im Personalsatz
- eingeschränkte Schreib- und Leseberechtigung für besondere Datenfelder (Gehalts- bzw. Stundensätze)
- Datenimportfunktion
- Zugriff auf Änderungs- und Logprotokolle

Auszug aus einer Rollenbeschreibung

Rollenbezeichnung	Beschreibung
PayAll	Änderung aller Personalstamm- und Bewegungsdaten/alle Abrechnungskreise (für Abteilungsleitung)
PayPflege01	Pflege der abrechnungsrelevanten Datenfelder ohne sensible Bereiche für Abrechnungskreis 01
PayBeweg	Pflege der monatlichen Bewegungsdaten für Abrechnungszwecke/alle Abrechnungskreise

Beispiel Rollendefinition

Datenfeld	Rolle PayAll	Rolle PayPflege	Rolle PayBeweg
PSNr	r/w	r	r
Name	r/w	r	r
Jahresurlaub	r/w	r/w	r
Gehalt	r/w	–	–
Stundensatz	r/w	r/w	–
Zeitdaten	r/w	–	r/w
Urlaubsabzug	r/w	–	r/w
Anwendungen	**Rolle PayAll**	**Rolle PayPflege**	**Rolle PayBeweg**
Abrechnung Testlauf	x	x	
Echtabrechnung	x	x	
DÜVO	x	x	

r = read (Leseberechtigung), w = write (Schreib- bzw. Änderungsrecht),
x = Ausführungsberechtigung

4. Prüfschritt: Vertretungsregelungen

Allzu oft gibt es keine sinnvolle Vertretungsregelung. Nicht selten wird der Benutzeraccount des Kollegen verwendet. Achten Sie darauf, dass jede Rolle möglichst zweimal zugeteilt wurde.

5. Prüfschritt: Batch-Anwendungen

Gerade bei der Personalabrechnung sind umfangreiche Batchläufe notwendig, um monatlich Daten zu verarbeiten und z.B. eine abschließende Lohn- und Gehaltsabrechnung zu erstellen.

Hier gilt es zudem zu prüfen, wer Batchläufe starten darf oder ob Regelungen für den Printoutput getroffen wurden. Weiter ist der datenschutzkonforme Datentransfer z.B. an die Sozialkassen zu prüfen.

Es gibt kein Patentrezept

Sie sehen am Beispiel der Entgeltabrechnung, welch umfangreiche Kontrollen nötig sind. Selbst für dieses Standardverfahren gibt es kein Patentrezept.

Mit den aufgezeigten Grundschritten sollten Sie jedoch in der Lage sein, weit komplexere Systeme wie z.B. SAP-Module zu prüfen. Viel Erfolg!

Hermann Keck