Komplexe Berechtigungskonzepte

Revision von SAP-Systemen

datenschutz nord GRUPPE

Komplexe Berechtigungskonzepte

SAP-Systeme sind sehr komplexe Software-Systeme, die in ihrer Gesamtheit kaum zu überschauen sind. Mögen SAP-Systeme kurz nach ihrer Einführung noch einigermaßen transparent sein, so stellt sich die Situation bereits nach mehrmonatigem Betrieb schon ganz anders dar: Die ursprünglich erstellte Dokumentation spiegelt den Wunschzustand wieder, nicht mehr den Ist-Zustand. Die unzähligen Systemparameter sind möglicherweise an einigen Stellen von verschiedenen Personen ohne nachvollziehbaren Grund verstellt worden; einzelne Benutzer haben mehr Zugriffsrechte als für die eigentliche Arbeit benötigt werden. Die Überprüfung, ob ein Benutzer wiederum ein bestimmtes Programm aufrufen darf oder nicht, stellt sich als ein baumartiges Geflecht von

- Berechtigungen
- Profilen bzw. Sammelprofilen
- Rollen und Sammelprofilen

dar und ist sehr komplex. Wir helfen Ihnen bei der Analyse dieser und weiterer sicherheitskritischer Aspekte und nutzen hierbei das SAP-eigene Audit-Informationssystem, um Fehleinstellungen und Schwachstellen zu erkennen und zu bewerten. Wir präsentieren Ihnen anschließend die Prüfungsergebnisse und geben Ihnen Handlungsempfehlungen zur Verbesserung der Sicherheit Ihrer SAP-Systeme.

---

preislich kalkulierbar

direkte Ansprechpartner

zeitlich kalkulierbar

ganzheitliches Projektmanagement

transparent

verständlich

Unsichere Auslieferung

Zugriffsrechte werden in Form von Authority-Checks in den ABAP/4-Programmen realisiert: Um auszuschließen, dass ein SAP-Benutzer Zugriff auf ein bestimmtes Datum hat, reicht es daher nicht aus, auf Datenbankebene den Zugriff auf das entsprechende Tabellenfeld zu verweigern. Es ist vielmehr notwendig, sämtliche Programme daraufhin zu überprüfen, ob der Authority Check dem Benutzer den Zugriff ermöglicht oder nicht. Um zu verhindern, dass Authority Checks in den Programmen verändert werden, ist eine Trennung von Test und Produktion umso wichtiger.

Um Benutzern nach einem Releasewechsel auch weiterhin einen reibungslosen Systemzugriff zu garantieren, wird ihnen in der Regel das Standard-Profil SAP_NEW zugeordnet, das den Zugriff für sämtliche hinzugekommenen Berechtigungsobjekte ermöglicht. Ohne entsprechende Modifikation des Profils SAP_NEW erhalten die Benutzer jedoch auch Zugriffsrechte für Objekte, die sie normalerweise nicht benötigen. Um zu verhindern, dass den Benutzern mittels SAP_NEW zusätzliche Zugriffsrechte eingeräumt werden, sollten die im Profil SAP_NEW enthaltenen und für den jeweiligen Releasewechsel benötigten zusätzlichen Berechtigungen in die jeweiligen Profile eingearbeitet werden.

In jedem SAP-Systems ist der Pseudobenutzer SAP* implementiert, der nicht gelöscht werden kann und uneingeschränkte Rechte auf das System hat. Eine Sicherung gegen eine unbefugte Nutzung dieser Kennung ist nur möglich, wenn in jedem Mandanten zu der Kennung SAP* ein Benutzerstammsatz angelegt wird, das Initialkennwort verändert und der SAP*-Kennung keinerlei Rechte zugewiesen werden. Allerdings besteht weiterhin das Risiko, dass der Benutzerstammdatensatz vom Datenbank-Administrator gelöscht und neu generiert wird.

Wie wird die Revision durchgeführt?

Die Revision von SAP-Systemen wird von unseren SAP-Spezialisten in enger Abstimmung mit Ihren SAP-Experten vor Ort durchgeführt. Die Revision umfasst sowohl das Basissystem als auch sicherheitsrelevante Module wie beispielsweise HCM (Human Resource) oder IS-H (Industry Solution Hospital).

Die Revision erfolgt in folgenden Schritten:

- Die zur Verfügung stehenden Dokumente, insbesondere das Freigabe-, Administrations- und Berechtigungskonzept werden von uns einer Vorabanalyse unterzogen.
- Die dabei gewonnenen Erkenntnisse sind Grundlage einer konzeptionellen Analyse sämtlicher sicherheitskritischer Aspekte (Basissystem, Module, Netzinfrastruktur, Server-Sicherheit) mit den SAP- und Netzwerkadministratoren vor Ort.
- Die konzeptionelle Analyse wird ergänzt um eine Auswertung von SAP-Reports, die Auskunft geben über SAP-Sicherheitsparameter, Trivial-Passwörter sowie vergebene sicherheitskritische Standard-Berechtigungen.
- In der konzeptionellen Analyse offen gebliebene Themen werden einer Detailanalyse vor dem System unterzogen. Dabei gilt es vor allem, Fehleinstellungen bei sicherheitskritischen Berechtigungen und Profilen zu erkennen.
- Die festgestellten Schwachstellen werden mit den SAP-Administratoren bewertet.
- Hieraus werden Vorschläge zur Verbesserung der SAP-Sicherheit unterbreitet. Diese Vorschläge können sich beispielsweise sowohl auf Rollen zur Benutzeradministration oder auf Anwendungsrollen beziehen.
- Sämtliche Prüfergebnisse werden in einer für den Auftraggeber verständlichen Form dokumentiert und präsentiert.

Woran sollte sich ein ordnungsgemäßer SAP-Betrieb orientieren?

Der SAP-Betrieb sollte ausreichend auch außerhalb des Systems in einem geeigneten Berechtigungs-, Administrations- und Freigabekonzept dokumentiert sein.

Es sollten getrennte Test- und Produktionsumgebungen eingerichtet sein. Der Transport von der Test- in die Produktivumgebung sollte durch entsprechende Transportaufträge und Freigaben erfolgen. Benutzerstammdatensätze sollten durch einen Benutzeradministrator, Berechtigungen durch einen Berechtigungsadministrator verwaltet werden. Die Fachmodule sollten von Moduladministratoren betreut werden. Das Berechtigungskonzept sollte sich möglichst an folgenden Gestaltungsprinzipien orientieren:

- Es sollten möglichst keine redundanten Berechtigungen vergeben werden, d.h. Rollen sollten möglichst nur in einer Sammelrolle enthalten sein.
- Es sollten möglichst keine Sammelrollen vergeben werden, die ihrerseits wiederum aus Sammelrollen bestehen.
- In der Produktionsumgebung sollten keine Standard-Rollen zum Einsatz kommen.
- In der Produktionsumgebung sollte auch das Standard-Profil SAP_NEW nicht zum Einsatz kommen. Die im Standard-Profil SAP_NEW enthaltenen Berechtigungen sollten in die bestehenden Profile integriert werden.
- Berechtigungen und Rollen sollten mit Hilfe des Profilgenerators vergeben werden.

Revision von SAP-Systemen – was kostet das?

Eine Revision von SAP-Systemen, die sich an den oben skizzierten Arbeitsschritten orientiert, führen wir einschließlich der Präsentation und Dokumentation der Arbeitsergebnisse in ca. 4–5 Arbeitstagen durch. Hierdurch wird gewährleistet, dass sämtliche grundlegenden Schwachstellen ermittelt und entscheidende Verbesserungsvorschläge formuliert sind. Falls gewünscht, können auf der Grundrevision weitere Spezialanalysen durchgeführt werden.

Ihre Kosten für die SAP-Revision sind in jedem Fall kalkulierbar, denn wir vereinbaren mit Ihnen einen Festpreis.

datenschutz nord Gruppe

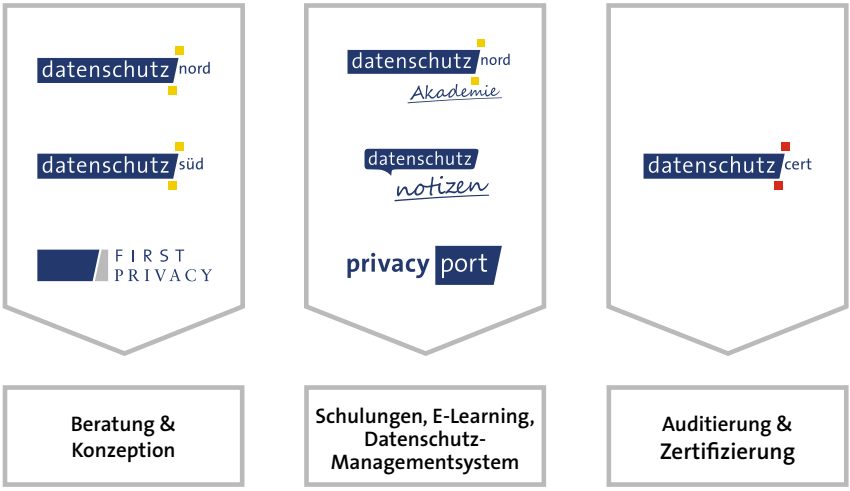
Zu der datenschutz nord Gruppe gehören die **DSN Holding GmbH,** deren Tochterunternehmen **datenschutz nord GmbH,** die **datenschutz süd GmbH,** die **datenschutz cert GmbH,** die international tätige **FIRST PRIVACY GmbH** sowie die **PRIVACY Central GmbH.**

Die datenschutz nord Gruppe ist einer der bundesweit führenden Dienstleister im Bereich Datenschutz. Bei mehr als 500 Unternehmen sind wir als externer betrieblicher Datenschutzbeauftragter tätig. Darunter sind klein- und mittelständische Unternehmen sowie Großkonzerne, sowohl Dienstleister als auch Produktionsunternehmen. Als Datenschutzbeauftragter sind wir zudem bei zahlreichen öffentlichen Stellen und kirchlichen Einrichtungen tätig.

Darüber hinaus beraten unsere IT-Sicherheitsexperten – lizenzierte ISO/IEC 27001- bzw. IT-Grundschutz-Auditoren – in allen Bereichen der Informationssicherheit. Wir erstellen **Sicherheitskonzepte,** führen **Penetrationstests** durch und entwickeln mit Ihnen gemeinsam ein für Ihr Unternehmen maßgeschneidertes **Informationssicherheits-Management.**

Mit der **datenschutz nord Akademie** bieten wir ein breites Spektrum an Schulungen an, welche als Präsenzseminare, Webinare und in Form von E-Learning Kursen besucht werden können. Mit unserem **Datenschutz-Managementsystem privacy port** können Sie Ihren Dokumentations- und Rechenschaftspflichten nachkommen und alle datenschutzrechtlichen Themen Ihres Unternehmens DSGVO-konform und übersichtlich verwalten. Seit Jahren informieren wir täglich und an zentraler Stelle auf unserem Blog **www.datenschutz-notizen.de** über Neuigkeiten rund um das Thema Datenschutz.

Unsere Geschäftsfelder



02/dsn

datenschutz nord GmbH

Hauptsitz Bremen
Konsul-Smidt-Straße 88
28217 Bremen
Tel.: +49 (0) 421 69 66 32-0

office@datenschutz-nord.de
www.datenschutz-nord-gruppe.de

datenschutz süd GmbH

Hauptsitz Würzburg
Wörthstraße 15
97082 Würzburg
Tel.: +49 (0) 931 30 49 76-0

office@datenschutz-sued.de
www.datenschutz-nord-gruppe.de

Weitere Niederlassungen der datenschutz nord Gruppe siehe **www.datenschutz-nord-gruppe.de/standorte**

datenschutz nord

datenschutz süd