Berechtigungsworkshop

Max Mustermann AG

Thema:

Analyse der Fileserver- und Berechtigungsstrukturen
Vorschläge und Wege zur Optimierung
Planung zur Einführung eines Daten-, Identitäts- und Berechtigungsmanagements

Termin:

Ihr Wunschtermin

Consultant:

Max Mustermann

aikux.com GmbH
Alt-Moabit 59-61
10555 Berlin

Geschäftsführer: Thomas Gomell
Tel.: +49 (30) 8095010-40
Fax: +49 (30) 8095010-41
Email: info@aikux.com

www.aikux.com

Inhalt

Ist-Situation 3
Ziele 4
Grundsätzliche Bewertung 5
Ergebnisblock / Maßnahmen-Summary 6
Vorrangige Maßnahmen 6
Grundlagen der Bewertung 7
Prozesse (Effizienz) 7
Datenschutz 7
Sicherheit 7
Dokumentation und Nachvollziehbarkeit 7
Bewertung der aktuellen Situation 8
Details, Bewertungen, Lösungsvorschläge 10
Klassifikation der Daten 10
Prozesse zur Berechtigungsvergabe 11
Struktur des Filesystems 12
Strategie - neues Berechtigungskonzept 13
Dokumentation und Nachvollziehbarkeit 13
Klassifizierung von Daten 13
Nächste geplante konkrete Schritte 14
Allgemeines Vorgehen und Standards 15
Weiterführende allgemeine Optimierungen 15
Step 0 – Aufbau und Definition der zukünftigen Prozesse 15
Step 1 – Vorbereitung 15
Step 2 – Gespräche mit den Data Ownern 15
Step 3 – Aufbau der neuen Verzeichnisstruktur mit migRaven 15
Step 4 – Aufbau der Archivstruktur 15
Step 5 – Schulung der Data Owner 15
Step 6 – Schulung des First-Level Supports 15
Allgemeine Empfehlungen 16
Schlussbemerkungen 16

Ist-Situation

Folgende Fragen stehen im Vordergrund:

- Welche Merkmale weisen das Unternehmen und sein Daten- und Berechtigungsmanagement auf?
- Was ist die Situation der Verzeichnis- und Berechtigungsstrukturen beim Kunden?
- Welche organisatorische Entwicklung bedingt möglicherweise die Situation der Verzeichnis- und Berechtigungsstrukturen?
- Dreht sich das Tagesgeschäft des Kunden um kritische Daten, die unter den Schutz nach DSGVO fallen? Wie hoch ist der aktuelle Schutz im Unternehmen für diese Daten?
- Was wurde im Rahmen des Workshops betrachtet, analysiert und besprochen?

…

Ziele

Folgende Fragen stehen im Vordergrund:

- Welche Themen wurden während des Workshops erörtert und als Zielstellungen definiert?
- Welche Maßnahmen wurden besprochen, um die Ziele zu erreichen?

…

Grundsätzliche Bewertung

Folgende Fragen stehen im Vordergrund:

- Was sind die schwerwiegendsten Probleme?
- Was sollten die wichtigsten Ziele sein?
- Was ist besonders aufgefallen?
- Bei welchen Themen gibt es hohes Optimierungspotenzial?
- Wie ist die Gesamtsituation das Unternehmen bzgl. Verzeichnis- und Berechtigungsstrukturen zu bewerten?

…

Ergebnisblock / Maßnahmen-Summary

Vorrangige Maßnahmen

Folgende Fragen stehen im Vordergrund:

- Welche Maßnahmen sollten aus Datensicherheitsgründen oder um die Aktualität/Standardisierung der IT-Infrastruktur zu wahren, unbedingt kurzfristig durchgeführt werden?
- Welche Maßnahmen sollten mittelfristig umgesetzt werden?
- Welche Empfehlungen gibt es für das Verzeichnis- und Berechtigungsmanagement?

…

Grundlagen der Bewertung

Der folgende Abschnitt erklärt, anhand welcher Kriterien der Consultant/ die aikux.com die Situation betrachtet und bewertet.

Prozesse (Effizienz)

Die richtigen Prozesse stellen einen wichtigen Punkt im Berechtigungswesen dar. Dabei sind nach unserer Erfahrung die folgenden Prämissen zu beachten:

…

Datenschutz

Sobald Daten erhoben werden, entsteht auch ein hohes Schutzbedürfnis. Dies ist vor allem der Fall, wenn es sich um personenbezogene Daten handelt.

…

Sicherheit

In der IT-Sicherheit unterscheidet man schon lange drei wesentliche Grundbedrohungen. Nämlich den Verlust der Verfügbarkeit, der Integrität und der Vertraulichkeit. In der späteren Diskussion kam unter dem Eindruck der fortschreitenden Technik zur Übertragung von Dokumenten und Urkunden noch die Grundbedrohung des Verlustes der Authentizität hinzu.

…

Dokumentation und Nachvollziehbarkeit

Die Dokumentation und die Nachvollziehbarkeit sind weitere wichtige Punkte. Es muss sichergestellt werden, dass man zu jedem Zeitpunkt in der Lage ist, zu jedem Account bzw. jeder Ressource eine Historie aller Änderungen (Anlage, Wechsel, Austritt usw.) einsehen kann.

…

Bewertung der aktuellen Situation

Auf Basis der zuvor genannten Betrachtungspunkte erfolgt die Einschätzung der Gesamtsituation anhand eines Ampel-Scores für die Bereiche Prozesse (Effizienz), Sicherheit, sowie Dokumentation und Nachvollziehbarkeit.
(Ampel Grün: gut, Ampel Gelb: normal, Ampel Rot: schlecht, Bewertungsgrundsatz: Das schwächste Glied bestimmt die Stärke der Kette)

aikux.com Score		
Prozesse	**Sicherheit**	**Dokumentation/ Nachvollziehbarkeit**
rot	grün	gelb

Die obige Bewertung erfolgt auf Basis folgender Fragestellungen, der Bereich **Datenschutz** wird von uns nicht **bewertet**, geht aber in die Betrachtung ein:

Prozesse (Effizienz):

Folgende Fragen stehen im Vordergrund:

- Sind die richtigen Leute in die Prozesse eingebunden?
- Wie viele Medienbrüche gibt es?
- Wie viel wird über Regeln und Automatismen abgebildet?
- Gibt es Standardisierung: z.B. über Rollen?
- Gibt es eine zwangsweise Überprüfung der Rechte durch Data Owner (Rezertifizierung)?
- Sind professionelle Tools im Einsatz, die die technische Umsetzung übernehmen?
- Gibt es Wege an den Prozessen vorbei?

Sicherheit:

Folgende Fragen stehen im Vordergrund:

- Wie wird mit der Aktivierung/ Deaktivierung von Accounts umgegangen?
- Wie ist der allgemeine Umgang mit Passwörtern?
- Wie ist die Ablage von Passwörtern und der Zugang zur zentralen Passwortdatenbank geregelt?
- Wie ist das Verfahren zum Passwort-Reset?

- Nach welchen Prinzipien werden die Berechtigungen vergeben?
- Wird nach dem Least-Privilege Prinzip gearbeitet?
- Auf wie vielen Verzeichnissen gibt es „Jeder“ oder „Authentifizierte Benutzer“ Berechtigungen?
- Auf wie vielen Verzeichnissen sind mehr als 10% der Benutzer berechtigt?
- Werden Rechte nach einem Abteilungs-/ Gesellschaftswechsel automatisch entzogen?

Dokumentation und Nachvollziehbarkeit:

Folgende Fragen stehen im Vordergrund:

- Gibt es ein einheitliches Logging?
- Gibt es Medienbrüche in den Prozessen?
- Ist die Dokumentation lückenlos?

Details, Bewertungen, Lösungsvorschläge

aikux.com Score		
Prozesse	**Sicherheit**	**Dokumentation/ Nachvollziehbarkeit**
rot	rot	rot

Klassifikation der Daten

Prozesse (Effizienz)

Folgende Fragen stehen im Vordergrund:

- Sind Prozesse für die Datenklassifizierung vorhanden und wenn ja welche?
- Funktionieren diese Prozesse?

Sicherheit

Folgende Fragen stehen im Vordergrund:

- Wird im Unternehmen mit kritischen Daten gearbeitet?
- Ist die Sicherheit dieser Daten gewährleistet und wenn ja, durch welche Maßnahmen?
- Sind diese Maßnahmen ausreichend?

Dokumentation und Nachvollziehbarkeit

Folgende Fragen stehen im Vordergrund:

- Wenn es eine Datenklassifizierung gibt, ist diese dokumentiert und nachvollziehbar?

Lösungsvorschläge

…

aikux.com Score		
Prozesse	**Sicherheit**	**Dokumentation/ Nachvollziehbarkeit**
gelb	gelb	gelb

Prozesse zur Berechtigungsvergabe

Prozesse (Effizienz)

Folgende Fragen stehen im Vordergrund:

- Gibt es Prozesse für die Berechtigungsvergabe und Rezertifizierung von Berechtigungen?
- Wer ist das Korrektiv für die Berechtigung zum Zugriff auf Daten des Data Owner?

Sicherheit

Folgende Fragen stehen im Vordergrund:

- Besteht ein Sicherheitsrisiko aufgrund von Vollzugriff/Überberechtigung/Admin-Rechten?
- Ist ein Berechtigungskonzept vorhanden oder haben alle Mitarbeiter auf alle Ordner Zugriff?

Dokumentation und Nachvollziehbarkeit

Folgende Fragen stehen im Vordergrund:

- Ist dokumentiert und nachvollziehbar, wer auf welches Verzeichnis wann und warum Zugriff hat?

Lösungsvorschläge

…

aikux.com Score		
Prozesse	**Sicherheit**	**Dokumentation/ Nachvollziehbarkeit**
rot	gelb	nicht relevant

Struktur des Filesystems

Prozesse (Effizienz)

Folgende Fragen stehen im Vordergrund:

- Welche Altersstruktur weisen die Verzeichnisse und Daten im Filesystem auf (Scan migRaven)?
- Wie hoch ist der hoch ist der Anteil Daten älter als zwei Jahre?
- Bis zu welcher Verzeichnisebene wurden Berechtigungen vergeben?
- Welche Dateitypen werden hauptsächlich im Filesystem abgelegt und welches Speichervolumen belegen diese?

Sicherheit

Folgende Fragen stehen im Vordergrund:

- Wie hoch ist die Wahrscheinlichkeit, dass der Verwaltungsaufwand zu hoch ist und dadurch Berechtigungen nicht korrekt gesetzt werden?

Dokumentation und Nachvollziehbarkeit
Nicht relevant – dieser Bereich ist für die Betrachtung der Situation nicht relevant.

Lösungsvorschläge
…

Strategie - neues Berechtigungskonzept

Folgende Fragen stehen im Vordergrund:

- Welche Strategie für das Daten- und Berechtigungskonzept wird empfohlen?
- Auf welchen Prozessen und Komponenten beruht es?
- Mit welchen Schritten und Maßnahmen kann ein neues Daten- und Berechtigungskonzept etabliert werden?
- Welche Verantwortlichkeiten und Softwarekomponenten sind notwendig?

Dokumentation und Nachvollziehbarkeit

Folgende Fragen stehen im Vordergrund:

- Wie können Change-Prozess nachvollziehbar dokumentiert werden?

Klassifizierung von Daten

Folgende Fragen stehen im Vordergrund:

- Warum sollten Daten klassifiziert werden und wie kann ein Klassifizierungsprozess sowohl auf dem Fileserver als auch in der Organisation implementiert werden?

Nächste geplante konkrete Schritte

Nachfolgend werden die Schritte genannt, die sich aus dem Workshop für die Zielerreichung des Unternehmens ergeben haben und eine erste Aufwandseinschätzung wird gegeben.

Arbeitsschritt	Dauer	Verantwortlichkeit
1. Vorbereitung		
…	2 h	aikux.com GmbH
…		
2. Kommunikation		
…		
…		
5. Inbetriebnahme		

Allgemeines Vorgehen und Standards

Folgende Fragen stehen im Vordergrund:

- Welches Standardvorgehen werden für die Bereinigung der Berechtigungen und der Reduzierung möglicher Sicherheitsprobleme angewendet?
- Welche Tools und Prozesse werden dafür implementiert?

Weiterführende allgemeine Optimierungen

Step 0 – Aufbau und Definition der zukünftigen Prozesse

…

Step 1 – Vorbereitung

…

Step 2 – Gespräche mit den Data Ownern

…

Step 3 – Aufbau der neuen Verzeichnisstruktur mit migRaven

…

Step 4 – Aufbau der Archivstruktur

…

Step 5 – Schulung der Data Owner

…

Step 6 – Schulung des First-Level Supports

…

Allgemeine Empfehlungen

Hier finden Sie allgemeine Empfehlungen zu Standards im Bereich Verzeichnis- und Berechtigungsmanagement mit Bezug zur Situation in Ihrem Unternehmen.

Alles hängt an guten Prozessen

In einem Unternehmen ist es wichtig, Prozesse zu etablieren. In den Daten liegt ein großer Teil des Unternehmensvermögens, …

Einfache Struktur bedeutet effektive Mitarbeiter

Je flacher eine Struktur ist – desto besser kann sie genutzt werden. Die heutigen Serversysteme bieten die Möglichkeit …

Nur Rechte setzen, die benötigt werden

Aus Gründen der Transparenz ist es sinnvoll nur dann Rechte zu vergeben, bzw. die Strukturen dafür nur dann vorzubereiten, wenn sie tatsächlich benötigt werden …

Archivierungskonzept

…

Schlussbemerkungen

…

Max Mustermann, 20.04.18