Otto-von-Guericke-Universität Magdeburg

Fakultät für Informatik

Bachelorarbeit

Konzept und Integration eines Privileged Identity Prozesses am Beispiel von ITP Panorama

Autor:

David Halm

2. August, 2013

Betreuer:

Prof. Dr. Hans-Knud Arndt

Institut für Technische und Betriebliche Informationssysteme

Halm, David:
Konzept und Integration eines Privileged Identity Prozesses am Beispiel von ITP Panorama
Bachelorarbeit, Otto-von-Guericke-Universität Magdeburg, 2013.

Inhaltsangabe

Administratoren und deren Aufgaben sind Teil eines jeden IT-Systems. Dabei sind die Anforderungen für Administratoren sehr hoch im Hinblick auf Geheimhaltungen von Daten. Es wird ein Regelwerk präsentiert, welches die Anforderungen beschreibt. Im Anschluss daran erfolgt eine Anwendung an dem Beispiel ITP Panorama, welches aufgrund von Analyse anderer Tools gewählt wurde. Aus diesen Erkenntnissen wird ein Modell für weitere Systeme erstellt und anhand eines Audits gezeigt, dass es den Anforderungen gerecht wird.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

CMMI	Capability Maturity Model Integration
ISMS	Managementsystem für Informationssicherheit
ISO	Internationale Organisation für Normung
ITIL	Information Technology Infrastructure Library
PIM	Privileged Identity Management
PKI	Public-Key-Infrastruktur

1. Einführung

Die Globalisierung ist ein wesentlicher Bestandteil vieler Firmen. Diese internationale Vernetzung hat nicht nur Vorteile wie neue Märkte oder Spezialisierungen, sondern auch Nachteile wie Cyberkriminalität. Dabei bezeichnet der Begriff Cyberkriminalität nach [BF11] die Kriminalität, die in Informations- bzw. Computersystemen stattfindet. Im Norton Cybercrime Report 2012[1], schätzt Norton für das Jahr 2012 den Schaden von Internetkriminalität auf 110 Milliarden US Dollar und in Deutschland auf 2,83 Milliarden Euro. Diese Schäden führen bei einigen Firmen dazu, ihre IT-Systeme auf Sicherheit zu überprüfen.

Die Volkswagen AG ist 2011 ihren Compliance Verpflichtungen[2] nachgekommen und hat ihre Prozesse unter dem Gesichtspunkt von IT Security überprüft. Aufgrund dieser Untersuchung wurde Handlungsbedarf festgestellt.

Bei der Recherche zu diesem Thema, wurde der Artikel im Anhang A.1 gefunden. Durch das Einstellen der "Financial Times Deutschland" [IQ8] ist nicht abzusehen, ob die Internetquelle weiterhin zur Verfügung steht. Deshalb wird der Originaltext des Internetauftrittes im Anhang A.1 abgebildet. Dieses wurde so entschieden, um zum einen den Kontext aus der Quelle weiterhin zur Verfügung zu haben und zum anderen, um bei nicht Verfügbarkeit der Quelle zu zeigen, dass hier nur der Bericht als Recherche diente.

Dieser Artikel wird nicht von der Volkswagen AG kommentiert.

Diese Arbeit bezieht sich auf das Projekt IT Administration Access Control, insbesondere auf das Thema Privileged Identity Management. Als Pilot für dieses Projekt diente das System DIALOGplus. Bei dieser Pilotierung wurden Defizite erkannt, welche abgebaut werden sollen.

[1] http://www.norton.com/2012cybercrimereport [IQ1]

[2] Compliance: "Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin" [IQ9]

1.1 Ziele

Ziel dieser Arbeit besteht darin ein Security Modell vorzustellen, es auf das System ITP Panorama anzuwenden, um daraus ein Modell abzuleiten wie man das Security Modell auf andere Systemkomponenten von DIALOGplus anwenden kann. Ein weiteres Ziel ist das Erreichen des CMMI-Levels 1 des CMMI Modells.

1.2 Gliederung der Arbeit

Diese Arbeit unterteilt sich in das Kapitel Grundlagen, in dem das CMMI Reifegradmodel, ITIL, Privileged Identity Management, das Security Modell und das System ITP Panorama beschrieben werden. [3]

Es folgt die Anwendung eines Regelwerkes, welches im Grundlagenteil vorgestellt wird, am Beispiel von ITP Panorama, mit Verbesserungsvorschlägen bei Defiziten.

Danach wird aus dieser beispielhaften Anwendung ein Konzept entwickelt, dass für weitere Systeme anwendbar sein soll.

Zum Schluß folgen ein Ausblick und eine Zusammenfassung der Arbeit.

[3] http://www.itp-panorama.com [IQ3]

2. Grundlagen

Im folgenden Kapitel werden die notwendigen Grundlagen für diese Arbeit beschrieben. Zunächst werden das Capability Maturity Model Integration (CMMI) vorgestellt, im Vordergrund steht hier der Reifegrad 1. Des Weiteren wird die Good-Practise Sammlung Information Technology Infrastructure Library (ITIL) vorgestellt. Dem folgend soll das Privileged Identity Management (PIM) beschrieben werden. Weiterhin wird das vorgegebene Security Modell vorgestellt. Abschließend wird das System ITP Panorama präsentiert.

2.1 CMMI

CMMI ist eine Zusammenfassung von Referenzmodellen zur Reifegradbestimmung und Verbesserung von Prozessen in Entwicklung von Produkten und dem Service. Aufgrund der Zielsetzung der Arbeit, das CMMI-Level 1 zu erreichen, wird nicht näher auf die anderen Reifegrade eingegangen.

Es werden nicht nur die Best-Practise von CMMI bereitgestellt, sondern auch die Schritte, die unternommen werden müssen, um diese in der Organisation einzuführen.

2.1.1 Die Reife- und Fähigkeitsgrade

CMMI bietet 2 unterschiedliche Darstellungsformen, die auf ganze Organisationen als auch einzelne Projekte angewendet werden kann. Diese 2 Formen sind Reifegrade und Fähigkeitsgrade. Dies hat den Vorteil, dass man einen Prozess in kleineren Projekten testen und später an die Organisationseinheit anwenden kann.

Tabelle 2.1 zeigt die 5 verschiedenen Reife- und 6 Fähigkeitsgrade. *Ein Reifegrad (engl. maturity level) ist der Grad der Prozessverbesserung in einem vordefinierten Satz von Prozessgebieten, in dem alle spezifischen und generischen Ziele erreicht werden.* [CKS09] *Ein Fähigkeitsgrad (engl. capability level) ist das erreichte Niveau der Prozessverbesserung innerhalb eines einzelnen Prozessgebiets. Ein Fähigkeitsgrad wird durch die entsprechenden spezifischen und generischen Praktiken für ein Prozessgebiet definiert.* [CKS09]

Die Unterteilung in Reifegrade wird zur phasischen Veränderung von Prozessen genutzt. Dabei bildet ein Reifegrad immer die Basis zum nächsthöheren Reifegrad, womit eine Reihenfolge zum Erreichen des höchsten Reifegrades 5 vorgegeben ist. Diese Darstellung ist nicht so flexibel, da man hier alle Prozessgebiete von CMMI beachten muss.

Die Darstellung in Fähigkeitsgraden ist flexibler zur Prozessverbesserung, da hier die Organisation entscheiden kann, in welchem Bereich sie sich verbessern will. Da diese Arbeit sich vor allem auf privilegierte Nutzer beschränkt, reicht es die Fähigkeitsdarstellung zu wählen.

Nachfolgend werden nur die Fähigkeitsgrade 0 und 1 erläutert, da die restlichen nicht relevant für diese Arbeit sind. Im weiteren Verlauf der Arbeit wird das CMMI-Level, mit dem Fähigkeitsgrad gleichgesetzt.

Fähigkeitsgrad 0: Unvollständig

Nach [CKS09] wird in dem Fähigkeitsgrad 0, ein Prozess nur teilweise oder gar nicht durchgeführt. Für diesen Grad gibt es keine Ziele, da es keine Gründe gibt, einen Prozess zu etablieren, der nur teilweise durchgeführt wird.

Fähigkeitsgrad 1: Durchgeführt

Prozesse mit dem Fähigkeitsgrad 1 sind durchgeführte Prozesse, die ein spezifisches Ziel und Arbeitsergebnisse verfolgen. Prozessverbesserungen können auftreten, werden aber nicht dauerhaft beibehalten. Dies geschieht erst durch die Institutionalisierung in den Fähigkeitsgraden 2 bis 5.

Grad	Darstellung in Fähigkeitsgraden	Darstellung in Reifegraden
0	Unvollständig	-
1	Durchgeführt	Initial
2	Geführt	Geführt
3	Definiert	Definiert
4	Quantitativ geführt	Quantitativ geführt
5	Prozessoptimierung	Prozessoptimierung

Tabelle 2.1: Reife- und Fähigkeitsgrade von CMMI

2.1.2 Auditierung von DIALOGplus

Bei der Volkswagen AG wurde das System DIALOGplus auditiert und mit dem CMMI-Level 0 bewertet. Dies bedeutet, dass die Prozesse innerhalb des Systems unvollständig, bzw. nicht ausgeführte Prozesse beinhalten. Es wurde z.B. kein Notfallkonzept gefunden oder die Administrator-Konten konnten nicht bestimmt werden.

Dies war der Anlass, die Systemkomponente ITP Panorama zu nutzen und mit deren Hilfe schrittweise das Komplettsystem DIALOGplus zu verbessern. Es sollen dabei vorrangig die privilegierten Konten bestimmt und überprüft werden.

2.2 ITIL

Die Information Technology Infrastructure Library (ITIL) wurde in den 80er Jahren erschaffen, um IT Organisationen für ihre Geschäftsausrichtung zu verbessern, indem es Good- und Best-Practises anbietet. Dies gelang erst mit der 2. Version 2001 auch bei deutschen Firmen. Seit 2007 existiert ITIL V3, welches 2011 ein Update auf ITIL Edition 2011 erhielt.

ITIL V3 besteht aus 5 Bänden: Service Strategy, Service Design, Service Transition, Service Operation und Continual Service Improvement.

2.2.1 Service Strategy

In dem Buch Service Strategy wird die Basis für die strategische Grundausrichtung und Bewertung von IT Services zur Unterstützung eines Business geschaffen. Es stellt somit Richtlinien und Grundlagenstrukturen für alle weiteren Phasen zur Verfügung.

Die wichtigsten Ziele sind:

- Strategy Management for IT Services: Entwicklung von Strategien für Service
- Service Portfolio Management: Verwaltung von Serviceportfolio
- Financial Management for IT Services: Koordination des Budgets
- Demand Management: Sicherstellung von ausreichend Kapazitäten für Service
- Business Relationship Management: Erfüllung der Bedürfnisse von Kunden

Dabei steht für Service Strategy die Business- und IT-Strategie immer im Mittelpunkt [nach KB12].

2.2.2 Service Design

Das Service Design hat zur Aufgabe die Kundenanforderungen zu ermitteln und diese in Service-Management-Lösungen zu überführen. Dabei steht es im Mittelpunkt, neue oder geänderte Services zur späteren Einführung in die Produktivumgebung zu entwickeln.

Folgende Prozesse findet man im Service Design:

- Design Coordination: Koordination von Prozessen, Aktivitäten und Ressourcen
- Service Catalogue Management: Entwicklung und Pflege eines Servicekatalogs
- Service Level Management: Abschluss von Service-Level-Vereinbarung und Entwurf von Services
- Capacity Management: Sicherstellung, dass ausreichend Kapazitäten für Services bereitstehen

- Availability Management: Verantwortlich für die Verfügbarkeit von Services
- IT Service Continuity Management: Sicherstellung von Wiederherstellung der Services im Katastrophenfall
- Supplier Management: Verwaltung vom Partner (Zulieferer) mit ihren gelieferten Services
- Information Security Management: Gewährleistung von IT-Sicherheit

Dabei muss das Service Design die Aspekte Funktionalität, Ressourcen und Planung berücksichtigen und erfüllen [nach KB12].

2.2.3 Service Transition

Die Service Transition baut Services auf und überführt diese in den operativen Betrieb. Es koordiniert dabei auch die Änderungen an Services.

Die wichtigsten Prozesse sind:

- Change Management: Steuerung aller Changes
- Service Asset and Configuration Management: Bereitstellung von Beziehungen und Informationen zu Configuration Items
- Knowledge Management: Verfügbarkeit von Informationen innerhalb der Organisation

Es beinhaltet zudem Systeme und Funktionen, um Releases[1] für den Kunden zu ermöglichen [nach KB12].

2.2.4 Service Operation

Die Service Operation stellt die effektive und effiziente Lieferung und den Support eines Service sicher. Es werden dabei auch die täglichen Prozesse kontrolliert, gesteuert und durchgeführt.

Die wichtigsten Prozesse sind:

- Event Management: Überwachung von Services und Filterung von Events[2]
- Incident Management: Verwaltung aller Incidents[3], sowie die Wiederherstellung des Services
- Problem Management: Nachhaltiges Lösen von Problems[4]
- Request Fulfilment: Bearbeitung von Service-Aufträgen, wie Standard-Changes[5]

[1] Release: Versionsbezeichnungen für Software
[2] Events: ein Ereignis, welches für das Management von Bedeutung ist
[3] Incident: ein ungeplantes Ereignis
[4] Problems: eine unbekannte Ursache für ein oder mehrere Incidents
[5] Standard-Changes: kleine Änderungen mit geringem Risiko, z.B. Passwortrücksetzung

- Access Management: Bewilligung von autorisierten Anwendern, bestimmte Services zu nutzen

Es werden außerdem Informationen für die kontinuierliche Verbesserung gesammelt und analysiert [nach KB12].

2.2.5 Continual Service Improvement

Die Continual Service Improvement identifiziert und implementiert Aktivitäten zu Verbesserungen von Services. Dabei wird aus den Erfolgen und Misserfolgen der Vergangenheit gelernt, womit die Services kontinuierlich angepasst und die Effektivität und Effizienz verbessert werden.

Der wichtigste Prozess ist der 7 Step Improvement Process mit folgenden Schritten:

- Identifikation der Strategie und Ziele
- Definition der Messung
- Erfassung der Daten
- Strukturierung der Daten
- Generierung von Informationen
- Aufbereitung und Präsentation der Informationen
- Problemidentifikation und Lösungen

Durch diese Schritte können einzelne Stufen erreicht werden, worauf die Organisation aufbauen kann [nach KB12]

2.2.6 Rollen in ITIL

In ITIL werden Rollen vergeben, damit Verantwortlichkeiten besser erkennbar sind und auch Aufgaben spezifiziert werden können. Da in ITIL V3 über 40 Rollen in den verschiedenen Phasen definiert sind, werden nachfolgend nur die wichtigsten für diese Arbeit aufgeführt und später in der Arbeit genauer definiert: [6]

- Compliance Manager: Verantwortlich dafür, dass Standards eingehalten werden
- Anwendungsentwickler: Verantwortlich für die Bereitstellung von Anwendungen zur Gewährleistung der IT-Services
- Service Owner: Verantwortlich dafür, dass die vereinbarten Services erbracht werden

[6] http://www.wiki-itil.de/Rollen_in_ITIL_V3 [IQ4]

2.3 Privileged Identity Management (PIM)

Durch die hohe Vertrauensstellung der Administratoren bei den Unternehmen, besaßen diese hohe Rechte mit einer geringen Kontrolle und Überwachung. Durch die Zunahme der IT-Systeme, dem Zugang zu wertvollen Geschäftsunternehmen mit privilegierte Accounts und dem leicht zu verdienendem Geld mit den Informationen, verschwindet das Vertrauen bei den Unternehmen. Aus diesem Grund entstanden Gesetze und Richtlinien zur lückenlosen Kontrolle der Administratoren, wie die ISO[7] 2700X-Familie. [8]

2.3.1 ISO 2700X-Familie

ISO 27000

Dieser Standard stellt einen Überblick über Managementsysteme für Informationssicherheiten (ISMS), grundlegende Prinzipien, Konzepte, Begriffe und Definitionen für ISMS bereit [nach BSI08].

ISO 27001

Dieser Standard gibt Empfehlungen zur Einführung, dem Betrieb und der Verbesserung eines Informationssicherheitsmanagementsystems und ermöglicht auch eine Zertifizierung [nach BSI08].

ISO 27002

Dieser Standard definiert ein Rahmenwerk für das Informationssicherheitsmanagement und enthält notwendige Schritte um dieses aufzubauen. Durch die Umsetzung dieser Empfehlungen kann man nach ISO 27001 zertifiziert werden [nach BSI08].

ISO 27005

Dieser Standard gibt einen Überblick und Empfehlungen zum Risikomanagement für Informationssicherheit [nach BSI08].

ISO 27006

Dieser Standard definiert Anforderungen an Zertifizierungsstellen [nach BSI08].

Weitere ISO 2700X-Normen

Es sind weitere ISO 2700X Normen geplant, die zur besseren Anwendbarkeit von ISO 27001 dienen sollen [nach BSI08].

2.3.2 Arten von Accounts

Abbildung 2.1 auf Seite 9 zeigt die verschiedenen Account-Arten. Dabei wird zwischen 5 verschiedenen Accounts unterschieden:

- Fachlicher Applikationsaccount: hierbei handelt es sich um Accounts, die keine weitreichenden Rechte besitzen, außer die Applikation nutzen zu können

[7] ISO: Internationale Organisation für Normung

[8] http://www.searchsecurity.de/themenbereiche/identity-und-access-management/user-management-und-provisioning/articles/294910/ [IQ5]

- Fachlicher Power-User: hierbei handelt es sich um Accounts mit erhöhten Kompetenzen wie z.B. Änderung von Rechten für die fachlichen Applikationsaccounts
- Applikations-Admin: hierbei handelt es sich um Accounts, die sich selbst und Anderen User-Rechte für diese Applikation zuteilen oder Freigabegrenzen ändern können
- Datenbank-Admin: hierbei handelt es sich um Accounts, die allgemein auf den Server Zugriff haben und deshalb außerhalb der Anwendung agieren können
- privilegierter Account: hierbei handelt es sich um einen Account, der im Katastrophenfall eingesetzt werden kann, um bspw. das System neu zu starten

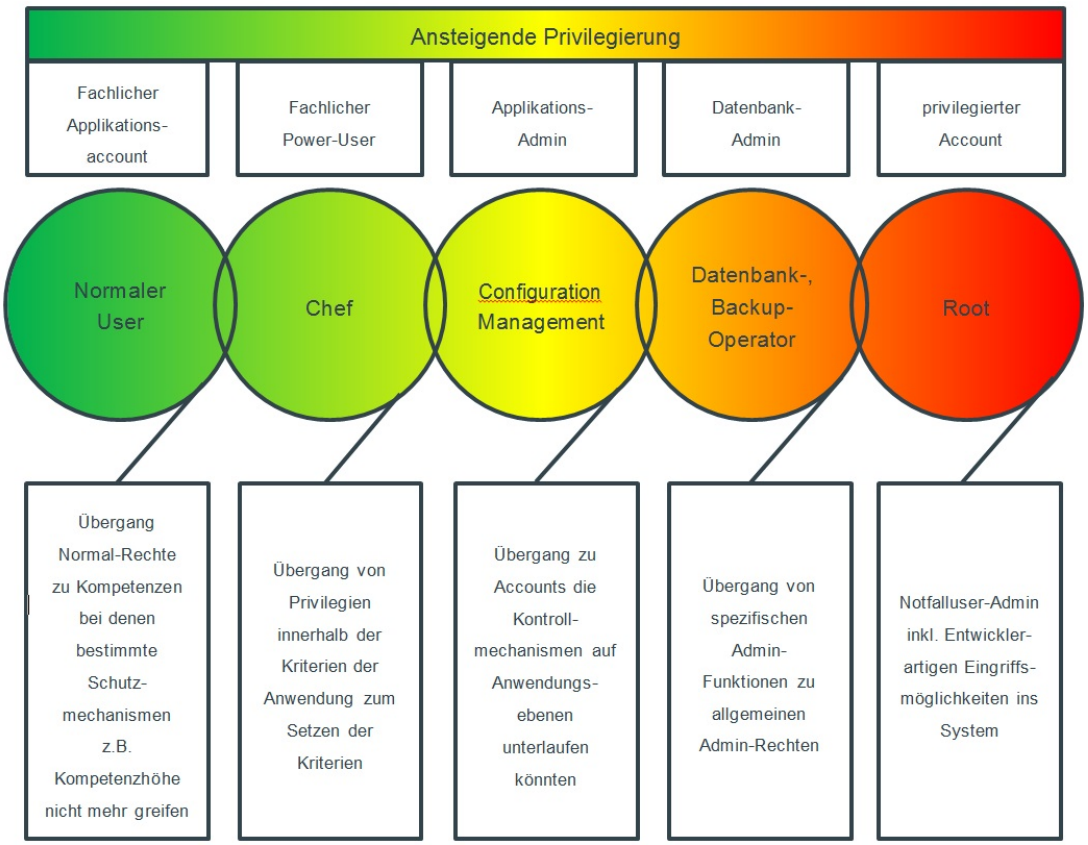


Abbildung 2.1: Account-Arten, eigene Bearbeitung nach [ITS11]

Man erkennt einen fließenden Übergang, wobei in der Praxis als entscheidende Privilegierung die Überschreitung von vorprogrammierten Leitplanken angesehen wird, da hier folgende Prinzipien nicht mehr technisch realisierbar sind: Funktionstrennung und Zugriffsbeschränkung. Erkennbar ist dieser Übergang vom Applikations-Administrator zum Datenbank-Administrator.

Aufgrund der Minimierung einer Gefahr mit privilegierten Accounts, wird meist eine neue User-ID angelegt, womit die Anzahl der Nutzer innerhalb einer Firma ansteigt, schnell unübersichtlich wird und bei Versetzung oder Ausscheiden des Mitarbeiters vergessen werden könnte. Es treten weitere Probleme mit privilegierten Accounts beim Austritt eines Mitarbeiters auf:

- Entfernen von privilegierten Rechten bei scheidenden Mitarbeitern
- Neues Zuweisen dieser Rechte auf andere Mitarbeiter, auf Grund von eventuellen Rollenkonflikten
- Zuweisen der neuen verantwortlichen Person
- Bei Übernahme eines Profils, die Passwortübergabe

Probleme bereiten auch die Shared Accounts, wo eine Gruppe von Administratoren Zugriff hat und somit keine Nachvollziehbarkeit vorhanden ist.

Für diese Probleme gibt es mehrere Lösungsansätze, wobei hier nur 2 behandelt werden: entweder muss eine regelmäßige Überprüfung der Accounts durchgeführt oder ein PIM-Lösung eingesetzt werden. Beide Lösungsansätze haben ihre Vor- und Nachteile und schließen sich grundsätzlich nicht gegenseitig aus. Die regelmäßige Überprüfung ist sehr zeitaufwändig und bei vielen Usern fehlerbehaftet. Dafür bietet es den Vorteil, dass der Nutzer sich an kein neues System gewöhnen muss. Die PIM-Lösung benötigt Vorarbeit, wie z.B. das CMMI Level 2. Durch die Überwachung von Administratoren bietet es den Vorteil, dass die gesetzlichen Vorschriften eingehalten und geschäftskritische Daten besser gesichert werden. Bei dieser Arbeit wird dem erstne Ansatz nachgegangen, um so die Vorarbeit für den 2. Lösungsansatz zu bieten.

2.4 Security Modell

Nach [BSI8] ist der IT-Grundschutz und somit die Sicherheit[9] gegeben, falls die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen nicht verletzt wird.

Vertraulichkeit ist gegeben, falls nur befugte Personen die Informationen bekommen.

Verfügbarkeit ist gegeben, wenn die Informationen dem Benutzer wie vorgesehen zur Nutzung bereitstehen.

Integrität ist gegeben, falls die Informationen vollständig und umgeändert zur Verfügung stehen.

In dem entwickelten Security Modell wird eine Gewaltenteilung angestrebt. Diese Gewaltenteilung besteht aus Executive (technisches Kompetenzfeld), Legislative (technisches Servicemanagement) und Judikative (Governance/Führungsebene). Im Kern des Modells steht das Security Center mit einem Regelwerk, welches nachfolgend vorgestellt wird.

Die Regeln für den Umgang mit privilegierten Rechten umfassen die folgenden Kernthemen:

Regel 1: Allgemeines

Regel 2: Dokumentation und Inventarisierung

Regel 3: Protokollierung

Regel 4: Authentisierung

Regel 5: Zyklische Überprüfung

Regel 6: Funktionstrennung

Regel 7: Besondere Accounts

Regel 8: Zugriff von außerhalb des Intranets

Regel 9: Notfalluser-Accounts

Nachfolgend wird jede Regel und die Maßnahmen zum Erreichen des Reifegrades 1 beschrieben [nach VW13].

2.4.1 Regel 1: Allgemeines

In allen IT-Bereichen des Volkswagen-Konzerns kommen Accounts mit administrativen und privilegierten Berechtigungen zum Einsatz. Die nachfolgenden Regeln haben das Ziel, die Sicherheit für diese besondere Gruppe der Accounts Schritt für Schritt und basierend auf bereits implementierten oder noch zu implementierenden Sicherheitsstandards zu erhöhen.

[9] Engl.: security

Im Rahmen eines abgestimmten, unternehmensweiten IT-Sicherheitskonzepts ist zunächst einmal das Vorhandensein eines PIM-Leitfadens mit integrierten Regeln, Maßnahmen und Controls zum Berechtigungsmanagement im Sinne der Compliance unerlässlich und vor dem Hintergrund zahlreicher gesetzlicher Bestimmungen zwingend erforderlich.

Um die in diesem Dokument genannten Maßnahmen umsetzen zu können, müssen folgende Dinge vorhanden sein:

- Prozesse zur Inventarisierung, Provisionierung und Dokumentation von Accounts
- Prozesse zur Rollen- und Berechtigungsvergabe
- Ein zentraler netzbasierter Authentisierungsdienst
- Eine Dokumentation aller operativen und funktionalen Rollen in den Geschäftsprozessen

Maßnahmen zu Regel 1

- Definition von geschäftskritischen IT-Services
- Schulung des Wartungs- und Administrationspersonals
- Sorgfältige Durchführung von Administrationstätigkeiten
- Sicherstellung einer konsistenten Systemverwaltung
- Sicherstellung einer konsistenten Datenbankverwaltung
- Sicherstellung einer konsistenten Netzwerkadministration
- Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
- Auswahl eins zentralen, netzbasierten Authentisierungsdienstes
- Sichere Verwaltung von Verzeichnisdiensten
- Einrichten und Konfigurieren von Zugriffsrechten auf Verzeichnisdienste
- Monitoring von Verzeichnisdiensten

2.4.2 Regel 2: Dokumentation und Inventarisierung

Die Regel 2 beinhaltet 3 Unterpunkte:

Erfassung und Überprüfung von administrativen und privilegierten Rechten

Für jedes IT-System müssen die privilegierten Accounts und deren Rechte detailliert erfasst werden. Jede Änderung an diesen Accounts ist ebenfalls zu protokollieren.

Die Aktualität der Accounts und Rechte muss in regelmäßigen Abständen überprüft werden.

Dokumentation von administrativen und privilegierten Rechten

Alle Accounts mit administrativen und privilegierten Rechten müssen vollständig (einschließlich des zugewiesenen Berechtigungsumfangs und der einzelnen zugewiesenen Rechte) erfasst und dokumentiert sein. Die Dokumentation muss aktuell gehalten werden. Für die gesamte Konzernstelle soll ein einheitliches Dokumentationssystem verwendet werden.

Rechte-Management

In jedem IT-System sind die Sessions der Accounts bei administrativen Tätigkeiten mindestens mit den systemeigenen Protokollierungsmöglichkeiten aufzuzeichnen.

Maßnahme zu Regel 2

Formblatt und Rechteprofile

- Erfassen aller personalisierten und nicht-personalisierten Accounts mit administrativen und privilegierten Rechten für alle IT-Systeme in schriftlicher Form
- Es muss eine begrenzte Anzahl von Rechteprofilen festgelegt werden. Ein neuer Benutzer wird dann einem solchen Profil zugeordnet und erhält damit genau die für seine Tätigkeit erforderlichen Rechte. Dabei sind die systemspezifischen Möglichkeiten bei der Einrichtung von Benutzern und Gruppen zu beachten.

2.4.3 Regel 3: Protokollierung

Um den ordnungsgemäßen Systembetrieb zu gewährleisten, sind die Tätigkeiten des Systemadministrators zu protokollieren, und zwar in einer Form, dass die Protokolle nicht durch den Systemadministrator oder Dritte verändert werden können.

Die Protokolle sind von unabhängigen Beschäftigten der Volkswagen AG angemessen zu überprüfen.

Maßnahme zu Regel 3

Auswertung der Logs

- Bei allen IT-Systemen, die über eine Logging-Funktion verfügen, ist diese aktiviert und wird für die Tätigkeiten der Accounts mit administrativen und privilegierten Rechten genutzt.
- Die Logs werden regelmäßig gesammelt und für einen festgelegten Zeitraum aufbewahrt.
- Die Logs werden bei Bedarf und sonst stichprobenartig überprüft.

2.4.4 Regel 4: Authentisierung

Sowohl für den Zutritt zu den IT-Systemräumen als auch für den Zugang zu IT-Systemen mit einem Administratoraccount bestehen zusätzliche Sicherheitsanforderungen für den Eintritts-/ Anmeldevorgang. Diese gehen über die Sicherheitsanforderungen für normale Anwenderaccounts hinaus.

Die Mindestanforderung für administrative Accounts mit Zugriff auf vertrauliche und geheime Daten sowie besonders geschäftsrelevante IT-Systeme, ist eine starke Authentifikation.

Maßnahme zu Regel 4

Anmeldung der Administratoren

- Alle Benutzer, die mit administrativen bzw. privilegierten Accounts arbeiten, melden sich mindestens mit Benutzername und Passwort an.
- Die administrativen bzw. privilegierten Accounts werden mehrheitlich personalisiert.
- Die Anzahl der nicht-personalisierten Accounts (Shared Accounts bzw. Built-in Accounts) wird, soweit technisch möglich, verringert.

Die Administratoren und privilegierten Nutzer müssen sich mit individuellem Nutzernamen und einem komplexen Passwort anmelden. Die Richtlinien für die Komplexität der Passwörter legt ein extra Regelwerk fest.

2.4.5 Regel 5: Zyklische Überprüfung

Alle Administrator-Accounts bzw. Accounts mit privilegierten Rechten müssen auf Grund ihrer im Vergleich zu normalen Anwender-Accounts umfangreicheren Berechtigungen, verbunden mit einem Zugriff auf besonders sicherheitsrelevante Daten, häufiger hinsichtlich Aktualität und Validität überprüft werden.

Ein regelmäßiger Überprüfungszyklus muss mindestens ein halbjährliches Review (einschließlich einer ggf. anschließenden Bereinigung) aller Zugänge mit administrativen und privilegierten Rechten in den IT-Systemen der Organisationseinheit/Konzerngesellschaft vorsehen. Zusätzliche Anlässe für ein Review außerhalb des regulären Zyklus können z. B. Systemwechsel, Patches, Updates, Changes etc. sein.

Maßnahme zu Regel 5

Review der administrativen Accounts

- Es wird ein einfacher Review-Prozess für Accounts mit administrativen bzw. privilegierten Rechten für die IT-Systeme eingeführt.
- Bei diesen Prüfungen werden abgelaufene bzw. langfristig inaktive Admin-Accounts identifiziert und kurzfristig gelöscht bzw. deaktiviert.
- Administrative Accounts, die für einen Zeitraum von 90 Tagen nicht mehr genutzt wurden, werden in den IT-Systemen deaktiviert.
- Die Änderungen werden nachvollziehbar dokumentiert und gesichert.

2.4.6 Regel 6: Funktionstrennung

Die Regel 6 beinhaltet 3 Unterpunkte:

Grundregel

Auf alle administrativen Tätigkeiten ist das Prinzip der Funktionstrennung anzuwenden, d. h. es muss mehr als eine Person erforderlich sein, um eine Prozessaufgabe abzuschließen. Zwischen den beteiligten Personen darf kein Unterstellungsverhältnis bestehen (z. B. darf die Person, die die Anlage eines administrativen bzw. privilegierten Accounts genehmigt, den Account nicht einrichten oder Admin-Rechte auf dem System besitzen). Dies gilt besonders für Tätigkeiten auf allen für die Aufrechterhaltung der Geschäftsprozesse relevanten IT-Systemen.

Dadurch wird gewährleistet, dass Fehler bzw. Missbrauch vermieden werden können.

Aufgabenteilung und Funktionstrennung

Die vom Unternehmen im Zusammenhang mit dem IT-Einsatz wahrzunehmenden Funktionen sind festzulegen. Zu unterscheiden sind hier zwei Ebenen:

- Die erste Ebene besteht aus den Funktionen, die den IT-Einsatz ermöglichen oder unterstützen, wie Arbeitsvorbereitung, Datennachbereitung, Operating, Programmierung, Netzadministration, Rechteverwaltung, Revision
- Die zweite Ebene besteht aus den Funktionen, die die zur Aufgabenerfüllung bereitstehenden IT-Verfahren anwenden. Beispiele solcher Funktionen sind: Fachverantwortlicher, IT-Anwendungsbetreuer, Datenerfasser, Sachbearbeiter, Zahlungsanordnungsbefugter

Im nächsten Schritt ist die Funktionstrennung festzulegen und zu begründen, d. h. welche Funktionen nicht miteinander vereinbar sind, also auch nicht von einer Person/einer Stelle gleichzeitig wahrgenommen werden dürfen. Vorgaben hierfür können aus den Aufgaben selbst oder aus gesetzlichen Bestimmungen resultieren.

Beispiel dafür ist: Programmierung und Test bei eigenerstellter Software

Vertreterregelung

Es muss für vorhersehbare (Urlaub, Dienstreise, etc.) und auch unvorhersehbare Fälle (Krankheit, Unfall, Kündigung, etc.) des Personenausfalls eine Vertretungsregelung etabliert werden, welche die Fortführung der Aufgabenwahrnehmung ermöglicht. Daher muss vor Eintritt eines solchen Falles geregelt sein, wer wen in welchen Angelegenheiten mit welchen Kompetenzen vertritt. Dies ist besonders im Bereich der Informationsverarbeitung von Bedeutung, da dafür meist Spezialwissen erforderlich ist und eine zeitgerechte Einarbeitung unkundiger Mitarbeiter für den Vertretungsfall nicht möglich ist.

Maßnahme zu Regel 6

Erfassung und Dokumentieren aller für die IT relevanten fachseitigen und IT-seitigen Funktionen

- Für die IT-Systeme der Organisationseinheit/Konzernstelle werden administrative Funktionen und Rollen mit kontrollierenden bzw. operativen Tätigkeiten identifiziert.
- Die administrativen Funktionen und Rollen werden beschrieben und dokumentiert.
- Die Listen mit den administrativen Funktionen und Rollen werden ausgewertet und Konflikte in der Funktionstrennung zwischen ausführenden und prüfenden Tätigkeiten werden identifiziert.

2.4.7 Regel 7: Besondere Accounts

Die Regel 7 beinhaltet 2 Unterpunkte:

Mindestanforderungen für Super-User-Accounts

Für alle Super-User-Accounts gelten Mindestanforderungen hinsichtlich der Sicherheit, welche über die der Accounts mit administrativen bzw. privilegierten Rechten noch hinausgehen. Alle in den IT-Systemen vorhandenen sogenannten Default-, Installations-, System- oder Service-Accounts dürfen keiner Person zugewiesen (personalisiert) werden und müssen entweder gelöscht, deaktiviert oder durch besonders lange und komplexe Passwörter geschützt werden.

Notfall-Accounts dürfen nur temporär aktiviert werden und sind mit einem zeitlich, auf die Dauer des Einsatzes limitierten, Passwort zu versehen.

Accountmanagement für generische bzw. Built-in Accounts auf Netzwerkinfrastrukturkomponenten

Alle generischen bzw. Built-in Accounts auf Komponenten der Netzwerkinfrastruktur (Router, Firewalls, Access Points etc.) müssen, entsprechend der Möglichkeiten des jeweiligen Systems und unter Berücksichtigung der Arbeitsfähigkeit, entweder entfernt, umbenannt, gesperrt/deaktiviert werden oder sind mit einem besonders komplexen Passwort zu sichern und unter Verschluss zu halten.

Maßnahme zu Regel 7

Erfassung, Dokumentation und Schutz von integrierten privilegierten Konten

- Besondere Accounts mit privilegierten Rechten werden für die UA/Konzernstelle für alle IT-Systeme erfasst und dokumentiert.
- Die besonderen Accounts werden durch höhere Sicherheitsvorkehrungen im Vergleich zu normalen Anwender-Accounts geschützt, bzw. unterliegen strengeren Auflagen, z.B. komplexeres Passwort, restriktivere Verwendung, kleinerer Kreis der Berechtigten, ausführlicheres Logging der Tätigkeiten im System etc.
- Die Umsetzung der Sicherheitsanforderungen wird dokumentiert und stichprobenartig überprüft.

2.4.8 Regel 8: Zugriff von außerhalb des Intranets

Ein administrativer Zugriff auf IT-Systeme von außerhalb des Intranets darf nur in einem gesonderten Sicherheitskontext stattfinden. Greift ein Mitarbeiter mit einem Administrator-Account bzw. einem Account mit privilegierten Rechten von außerhalb des VW-Intranets/Firmennetzes mit mobilen Zugangsgeräten auf interne IT-Systeme zu (z. B. zum Zweck der Fernwartung, Telearbeit u. ä.), sind spezielle Mindestsicherheitsanforderungen hinsichtlich Verschlüsselung, VPN-Tunnel, Session-Dauer usw. einzuhalten.

Als langfristige Lösung ist eine Absicherung von externen Zugriffen auf Basis eines Privileged Identity Management (PIM)-Systems und die Anwendung eines Mobile Device Managements umzusetzen.

Maßnahme zu Regel 8

Erfassung und Review von administrativen Konten mit Fernzugriff

- Die Anzahl der Accounts mit administrativen bzw. privilegierten Rechten, die eine Fernwartung durchführen, sowie die IT-Systeme, für die eine Fernwartung eingerichtet sind, werden erfasst und dokumentiert.

2.4.9 Regel 9: Notfalluser-Accounts

Vor dem Einrichten eines Notfalluseraccounts in einem IT-System, ist in einem Prozessdokument mindestens schriftlich Folgendes zu definieren:

- Was ist ein Notfall,
- Wer wann den Notfall-User Account verwenden/aktivieren darf,
- Wie das (Einmal-)Passwort eingerichtet (Länge, Komplexität) wird,
- Wie es sicher (z. B. versiegeltes Passwort im Umschlag im Tresor) unter Verschluss zu halten ist,
- sowie der Einsatz und die Aktivitäten des Accounts zu protokollieren und zu dokumentieren sind.

Nach dem Einsatz ist der Notfalluser-Account umgehend wieder zu deaktivieren.

Maßnahme zu Regel 9

Es wird ein Verfahren zur Definition eines Notfalls, zur Aktivierung des Notfall-User-Accounts und zur Dokumentation des Einsatzes erstellt und beschrieben.

2.5 System ITP Panorama

ITP Panorama ist ein von ITP entwickeltes Tool zur Analyse, Reengineering[10], Wartung, Weiterentwicklung und Nachdokumentation von großen Host-Programmsystemen. Dabei werden die relevanten Programmteile per Datenübertragung zu dem PANORAMA Server übertragen. Auf diesem Server findet der Scan statt und stellt diese aufbereiteten Informationen in Hypercubes[11] allen Arbeitsplätzen zu Verfügung. Daraus ergibt sich der Vorteil dass die Arbeitsplatzrechner wenig beansprucht werden.

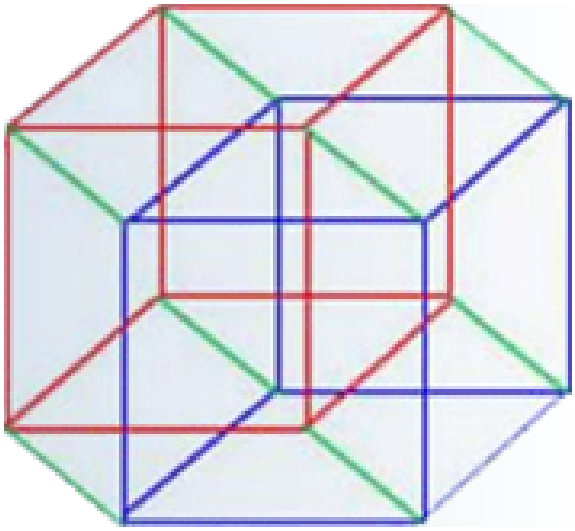


Abbildung 2.2: Hypercube, von [IQ3]

Bei komplexen Programmen können mit diesem Tool schnell Abhängigkeiten erkannt und daraus resultierend die Qualität verbessert werden. Weitere Einsatzmöglichkeiten sind: Einarbeitung neuer Mitarbeiter zu bestehenden Systemen, interaktive Weiterentwicklung wie z.B. EURO-Umstellung, Fehlersuche, Vollständigkeitsüberprüfung oder Überprüfung auf toten Code[12].

Durch eine Datenfluss-Analyse lässt sich die Wertschöpfungskette durch die Anwendungen und Programme verfolgen. Darüber hinaus wird der Hypercube nächtlich automatisch neu gebaut, womit das Aufbauen tagsüber vermieden wird und täglich ein aktualisierter Stand der Sourcen vorliegt. [nach IQ3]

[10] Reengineering: Software wird bei gleicher Funktionalität verbessert
[11] Hypercube: mehrdimensionaler Würfel
[12] toter Code: nicht ausführbarer Quelltext

3. Analyse und Konzeption

In diesem Kapitel soll die aktuelle Securityqualität im Kontext des Privileged Identity Management (PIM) im Projekt ITP Panorama analysiert werden. Das Ziel für das Projekt ist das Erreichen des CMMI-Level 1. Dazu werden die im Regelwerk gegebenen Regeln untersucht und bewertet. Hierzu wird jede Maßnahme analysiert und dazu die aktuelle Situation im Projekt ITP Panorama gezeigt. Anschließend wird die aktuelle Situation anhand einer Tabelle zusammengefasst und die Erfüllung (grün) und die nicht Erfüllung (rot) aufgezeigt. Bei den nicht erfüllenden Situationen wird die zukünftige Umsetzung gezeigt, um den Maßnahmen gerecht zu werden.

In der Regel 1 werden Grundvoraussetzungen geschaffen, wie die Sicherstellung einer konsistenten Netzwerkadministration oder die sorgfältige Durchführung von Administrationstätigkeiten. Diese Grundvoraussetzungen können nur schwer überprüft werden und gelten somit als gegeben.

3.1 Aktuelle Situation

Nachfolgend wird die aktuelle Situation des Projektes ITP Panorama mit Hilfe des Regelwerkes beschrieben.

3.1.1 Regel 1

Die Regel 1 wurde aus dieser Analyse ausgeschlossen, da diese Maßnahmen allgemein über alle Systeme handelt und es nicht speziell auf ein System untersucht werden kann. Zum Beispiel kann man nicht an einem System überprüfen, ob die Netzwerkadministrationen konsistent sind. Somit zählen diese Maßnahmen alle als gegeben für diese Untersuchung.

3.1.2 Regel 2

Die Maßnahmen für Regel 2 geben vor, dass man alle personalisierten und nichtpersonalisierten Accounts mit privilegierten Rechten für alle IT-Systeme erfasst. Für das CMMI-Level 1 reicht es aus, nur für das zu untersuchende System diese Accounts

aufzulisten. Es sollen außerdem eine begrenzte Anzahl von Rechteprofilen festgelegt und jedem Nutzer ein Profil zugeordnet werden.

Derzeitig betreuen 2 Personen das System ITP Panorama mit privilegierten Rechten und diese sind auch dokumentiert. Systemspezifisch muss jeder User einzeln einem Hypercube zugewiesen werden. Die Rechte für einen Hypercube sind einem Grundprofil zugeordnet. In diesem Grundprofil ist es erlaubt den Hypercube zu lesen. Es lassen sich mit einem Statistik-Profil zusätzlich noch die Statistiken zu dem Hypercube anzeigen.

Bezeichnung	Erfüllung
Erfassen privilegierte Accounts	
Rechteprofile für Nutzer	

Tabelle 3.1: Zusammenfassung Regel 2

3.1.3 Regel 3

Die Maßnahmen für Regel 3 geben vor, dass man bei allen IT-Systemen, die über eine Logging-Funktion verfügen, diese aktiviert. Für das CMMI-Level 1 reicht es aus, nur für das zu untersuchende System diese Log-Funktion zu aktivieren. Es sollen außerdem die Logs gesammelt und befristet aufbewahrt werden. Zuletzt sollen die Logs bei Bedarf und stichprobenartig überprüft werden.

Die Software ITP Panorama bietet derzeitig keine Logging Funktion für privilegierte Rechte. Dies liegt am lesenden Konzept der Software, womit jeder nur lesenden Zugriff hat. Dieser lesende Zugriff wird geloggt und gespeichert. Die Dauer der Speicherung wurde noch nicht festgelegt. Es werden bei Bedarf, z.B. Feststellung der Nutzerakzeptanz, diese Logs überprüft.

Privilegierte Nutzer haben Zugänge direkt zum Server, worauf sie besondere Rechte, wie einrichten neue Nutzer für bestimmte Hypercubes, haben. Dieser Zugang wird derzeitig nicht geloggt, womit auch diese nicht überprüft werden können.

Bezeichnung	Erfüllung
Logging-Funktion für privilegierte Nutzer aktiv	
Befristete Aufbewahrung der Logs	
Überprüfung der Logs	

Tabelle 3.2: Zusammenfassung Regel 3

3.1.4 Regel 4

Die Maßnahmen für Regel 4 geben vor, dass privilegierte Nutzer sich mindestens mit Benutzername und Passwort anmelden müssen. Es sollen die privilegierten Accounts soweit wie möglich personalisiert und die nicht-personalisierten Accounts verringert werden.

Die privilegierten Nutzer benötigen zur Anmeldung am Server einen Benutzernamen und ein Passwort. Derzeitig sind alle privilegierten Accounts personalisiert. Für das System ITP Panorama existiert kein nicht-personalisierter Account.

Bezeichnung	Erfüllung
Anmeldung mit Benutzername und Passwort	
Personalisieren der privilegierten Accounts	
nicht-personalisierte Accounts verringern	

Tabelle 3.3: Zusammenfassung Regel 4

3.1.5 Regel 5

Die Maßnahmen für Regel 5 geben vor, dass ein einfacher Review-Prozess für privilegierte Accounts eingeführt wird. Bei dieser Prüfung sollen inaktive oder abgelaufene Accounts identifiziert und deaktiviert werden. Diese Änderungen sollen dokumentiert werden.

Derzeitig gibt es für das Projekt ITP Panorama keinen Review-Prozess für privilegierte Accounts. Dies hängt damit zusammen, dass es nur 2 privilegierte Accounts gibt. Es gibt auch keine Überprüfung inaktiver privilegierter Accounts. Änderungen bei den privilegierten Accounts werden dokumentiert.

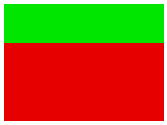
Bezeichnung	Erfüllung
Dokumentation bei Änderungen	
Review-Prozess	
Deaktivierung inaktive privilegierter Accounts	

Tabelle 3.4: Zusammenfassung Regel 5

3.1.6 Regel 6

Die Maßnahmen für Regel 6 geben vor, dass privilegierte Accounts mit kontrollierenden bzw. operativen Tätigkeiten identifiziert werden. Diese Rollen sollen beschrieben und dokumentiert werden. Aus dieser Dokumentation sollen Konflikte in der Funktionstrennung zwischen ausführenden und prüfenden Tätigkeiten identifiziert werden.

Es existieren 8 verschiedene Rollenprofile für ITP Panorama, wobei nicht alle Profile untereinander konfliktfrei sind. Diese Rollenprofile sind derzeit beschrieben, müssen aber noch abgestimmt werden. Durch die fehlenden Funktionsbeschreibungen kann keine Identifikation von Konflikten stattfinden.

Bezeichnung	Erfüllung
Identifizierung von Rollenprofilen	
Dokumentation der Rollen	
Identifikation von Konflikten	

Tabelle 3.5: Zusammenfassung Regel 6

3.1.7 Regel 7

Die Maßnahmen für Regel 7 geben vor, dass für alle IT-Systeme besondere Accounts mit privilegierten Rechten erfasst und dokumentiert werden. Hierbei sind die Built-In Accounts bei den Systemen gemeint, wie z.B. der Administrator Account bei

Microsoft Windows. Um den CMMI-Level 1 zu erhalten, ist es nur notwendig dies für ITP Panorama zu erfassen und zu dokumentieren. Es wird gefordert, dass diese Accounts besser geschützt sind und diese Sicherheitsanforderungen dokumentiert und stichprobenartig überprüft werden.

Für ITP Panorama ist ein Built-In Account eingerichtet und dieser wird von Microsoft Windows Server dokumentiert. Die Sicherheitsanforderungen sind dabei ein komplexes Passwort und ein kleiner Kreis der Berechtigten. Eine Dokumentation über die Sicherheitsanforderungen existiert nicht.

Bezeichnung	Erfüllung
Built-In Accounts dokumentieren	
höhere Sicherheitsanforderungen	
Dokumentation und Überprüfung der Sicherheitsanforderungen	

Tabelle 3.6: Zusammenfassung Regel 7

3.1.8 Regel 8

Die Maßnahmen für Regel 8 geben vor, dass die privilegierten Accounts, die für eine Fernwartung eingerichtet sind, dokumentiert sind. Um den CMMI-Level 1 zu erhalten, ist es nur notwendig dies für ITP Panorama zu erfassen.

Für ITP Panorama sind keine privilegierten Accounts mit Fernwartung eingerichtet.

Bezeichnung	Erfüllung
Dokumentation privilegierter Accounts mit Fernwartung	

Tabelle 3.7: Zusammenfassung Regel 8

3.1.9 Regel 9

Die Maßnahmen für Regel 9 geben vor, dass der Einsatz eines Notfallnutzerprozesses eingeführt und nachgewiesen werden kann.

Das Projekt ITP Panorama besitzt keinen Notfall-User-Account, da die Software nur lesenden Zugriff hat. Bei einem Ausfall der Server wird der Notfallnutzerprozess in einer anderen Abteilung ausgelöst.

Bezeichnung	Erfüllung
Dokumentation eines Notfallnutzerprozesses	

Tabelle 3.8: Zusammenfassung Regel 9

3.2 Verbesserungsvorschläge

Dieser Abschnitt soll die Verbesserungen der aktuellen Situation beschreiben, um den CMMI-Level 1 zu erhalten. Dafür werden alle Maßnahmen, die nicht erfüllt wurden, verbessert.

Um die Maßnahmen für Regel 3 zu erfüllen, muss die serverseitige Logging-Funktion aktiviert werden. Diese Logs sollten mindestens bis zum nächsten Audit aufbewahrt werden. Eine Überprüfung der Logs muss mindestens bei Verdachtsmomenten durchgeführt werden. Es wird aber, aufgrund von Erfahrungen aus anderen Systemen, empfohlen, alle 4 Wochen diese Logs zu überprüfen.

Um die Maßnahmen für Regel 5 zu erfüllen, muss ein Review-Prozess für die privilegierten Accounts eingeführt werden. Hierzu wird empfohlen, das quartalsweise diese Accounts überprüft und dokumentiert werden. Bei diesem Review muss geprüft werden, ob die Accounts noch gebraucht werden (Validität) und ob die vergebenen Rechte noch aktuell notwendig sind (Aktualität). Falls die Validität nicht gegeben ist, muss dieser Account deaktiviert werden. Ist die Aktualität nicht gegeben, muss das Rechteprofil des Nutzers angepasst werden. Die Dokumentation sollte vor Veränderungen geschützt werden und sollte deswegen verschlüsselt abgelegt werden.

Um die Maßnahmen für Regel 6 zu erfüllen, müssen die 8 Rollenprofile dokumentiert werden. Nach der Dokumentation müssen Konflikte hinsichtlich der Funktionstrennung gekennzeichnet werden. Diese beiden Punkte werden im Kapitel Konzept für weitere Systeme wieder aufgegriffen.

Um die Maßnahmen für Regel 7 zu erfüllen, ist die Empfehlung alle 3 Monate diese Built-In Accounts durch die IT zu überprüfen und zentral in einem Standardformat gesichert abzulegen. Nicht mehr benötigte Rechtezuweisungen sind zu löschen und es ist zu prüfen, ob die Nutzung der Built-In Accounts ggf. durch neue Releases der Hardware oder Software zukünftig ganz vermieden werden kann. Weiterhin ist eine Dokumentation der Sicherheitsanforderung anzufertigen, falls diese abweichend von Standards sind.

3.3 Modell für weitere Systeme

In diesem Abschnitt wird ein Konzept zur Erfüllung des Regelwerkes vorgestellt. Dabei wird, mit Ausnahme von Regel 1, für jede Regel eine Tabelle bereitgestellt, die für das jeweilige System ausgefüllt werden muss. Dieses wurde so gewählt, um die Komplexität der Tabelle so gering wie möglich zu halten und um den Fortschritt für jede Regel separat erkennbar zu machen. Regel 1 wird nicht betrachtet, da es die Grundlagen darstellt, die ein System als Solches nicht beeinflussen kann, wie die Regularien für Schulungen von Administratoren. Deshalb wird diese Regel als gegeben angesehen. Zusätzlich zu den Tabellen, werden bei den Fragenkatalogen die Mindestanforderungen erklärt, die erfüllt sein müssen um CMMI-Level 1 zu erreichen. Bei den restlichen auszufüllenden Tabellen ist diese korrekt und vollständig auszufüllen.

Die Tabellen sollen so gestaltet werden, dass sie für spätere Arbeiten für CMMI-Level 2 und 3 problemlos erweitert werden können. Zur besseren Lesbarkeit werden die Tabellen und Fragenkataloge transponiert dargestellt.

Die Betrachtung wurde dabei erweitert. Es wurde jetzt nicht nur das System ITP Panorama betrachtet, sondern das System ITP Panorama im Kontext von DIALOGplus. Dies wurde getan, um mehr Informationen für das Modell zu bekommen.

3.3.1 Deckblatt

In dem Deckblatt sollen grundlegende Informationen eingetragen werden. Hierzu zählen der Name des Systems, das Erstellungsdatum, der Systemverantwortliche, sowie der Autor. Weiterhin soll das System in einer der 4 Arten der Klassifizierung, öffentlich, intern, vertraulich und geheim, eingeordnet werden. Dies ist notwendig für die Auditoren, damit diese daraus erkennen, ob die berechtigten Personen Zugriff auf das System erhalten dürfen. Ein weiteres Feld ist die Anzahl der privilegierten Nutzer. Dieses wird benötigt um für Systeme mit kleinerem Nutzerkreis Arbeit zu ersparen, da man bei geringerer Anzahl von Personen den Grund für die privilegierten Rechte aus dem Antrag ableiten kann. Dieses macht nur bei kleineren Gruppen, hier definiert für bis zu 50 Personen, Sinn, da sonst der Verwaltungsaufwand für diese Anträge enorm steigt. Zum Schluss soll eine Zusammenfassung des Systems eingetragen werden. Auf dem Deckblatt werden der Inhalt der weiteren Tabellen, sowie die Dokumentenhistorie abgebildet.

In Abbildung 3.1 wird das zum Teil ausgefüllte Deckblatt für das System ITP Panorama im Kontext von DIALOGplus abgebildet.

Titel	Vorlage für das Regelwerk für das ITSP 4.4 Programm zur Erreichung von CMMI-Level 1	
System	ITP Panorama	
Klassifizierung	vertraulich	
Anzahl privilegierter Nutzer	15	Grund für privilegierte Rechte ist dem Antrag zu entnehmen
Datum		
Systemverantwortung	n N1	
Autor	n N2	
Zusammenfassung	Das Tool ITP-Panorama der ITP Software GmbH unterstützt die aktuelle Bereitstellung technischer Dokumentationen von komplexen IT Systemen. Die Software wurde in DB2- und COBOL-Projekten bei der Volkswagen AG und Audi AG eingeführt. Sie dient zur Analyse von Source-Code, der schnellen Dokumentation und einfachen Einarbeitung von Mitarbeitern in die unterstützten Systeme.	

Inhalt	
Seite/ Tabelle	**Zusammenfassung**
Deckblatt	Deckblatt für die Vorlage
Regel 2	Auflistung der privilegierten Accounts (inkl. Fernwartung)
Regel 3	Logging-Funktion
Regel 4	Anmeldung für privilegierte Accounts
Regel 5	Review-Prozess für privilegierte Accounts
Regel 6	Funktionstrennung
Regel 7	Sicherheitsvorkehrungen für privilegierte Accounts
Regel 8	Fernwartungsaccounts
Regel 9	Notfall-User

Historie des Dokumentes			
Version	**Datum**	**Autor**	**letzte Änderung**
0,1		n N3	initiale Version

Abbildung 3.1: Konzept für Deckblatt

3.3.2 Regel 2

Die Regel 2 befasst sich mit der Dokumentation aller privilegierten Accounts für das System. Hierzu sind der Login-Name, sowie die dazugehörige Person, zu dokumentieren. Falls der Login ein Built-In-Account ist, muss dies gekennzeichnet werden. Weiterhin muss gekennzeichnet werden, ob dieser Account zu einer internen oder externen Person gehört. Dieses ist wichtig zur Überprüfung der Klassifizierung, z.B. darf ein System, welches als geheim klassifiziert wurde, keine Accounts von externen Personen haben. Es sollen außerdem die Erreichbarkeit der Person und die zugehörige Organisationseinheit eingetragen werden. Es muss auch abgebildet werden, wann dieser Account angelegt wird, um bei automatisch aktualisierenden Systemen diese Accounts auch entsprechend deaktivieren zu können. Es muss auch dokumentiert werden, wogegen man sich anmelden muss, z.B. lokales Windows. Als Letztes ist der Grund für die Rechte auszufüllen. Dies ist bei Systemen mit weniger als 50 Accounts nicht notwendig, da man den Grund ohne viel Aufwand vom Antrag ableiten kann. Bei mehr als 50 Personen für das System, muss dies eingetragen werden, damit der Auditor schnell ableiten kann, ob die Berechtigung begründet ist.

Aus datenschutzrechtlichen Gründen, wird in dieser Arbeit nur das Konzept abgebildet und nicht die für ITP Panorama ausgefüllte Tabelle.

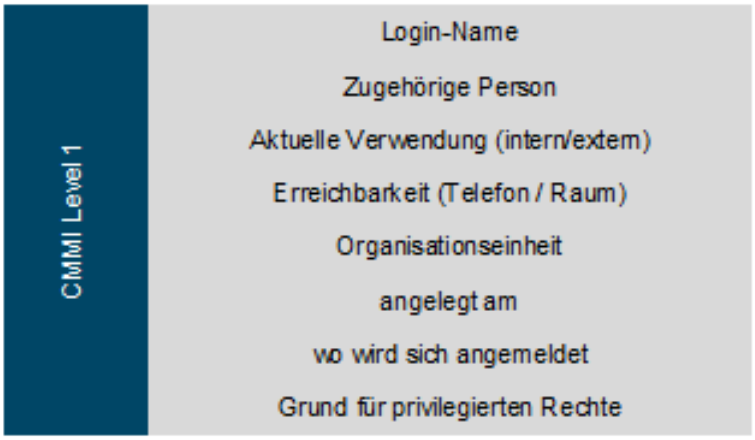


Abbildung 3.2: Konzept für Regel 2

3.3.3 Regel 3

Die Regel 3 befasst sich mit der Protokollierung von administrativen Arbeiten. Um CMMI Level 1 zu erfüllen, wurde hierzu ein Fragenkatalog erstellt und zusätzlich die Mindestanforderungen vorgegeben. Zu diesem Fragenkatalog gehören, ob eine Logging-Funktion vorhanden ist und wenn, ob sie aktiv ist. Falls diese nicht aktiv ist, muss begründet werden, warum sie nicht aktiv ist. Es muss weiterhin die Aufbewahrungsfrist dieser Logs, das Überprüfungsintervall und wer die kontrollierende Person hierfür ist, dokumentiert werden. Die Mindestanforderungen für ein System ohne Logging-Funktion, ist nur die Dokumentation, das diese nicht vorhanden ist. Die Mindestanforderung für Systeme mit Logging-Funktion ist, dass diese aktiv ist, die Aufbewahrungsfrist mindestens bis zum nächsten Audit beträgt und das es stichprobenartig durch den Compliance Manager überprüft wird.

Abbildung 3.3 zeigt den ausgefüllten Fragenkatalog, nach der Verbesserung von ITP Panorama.

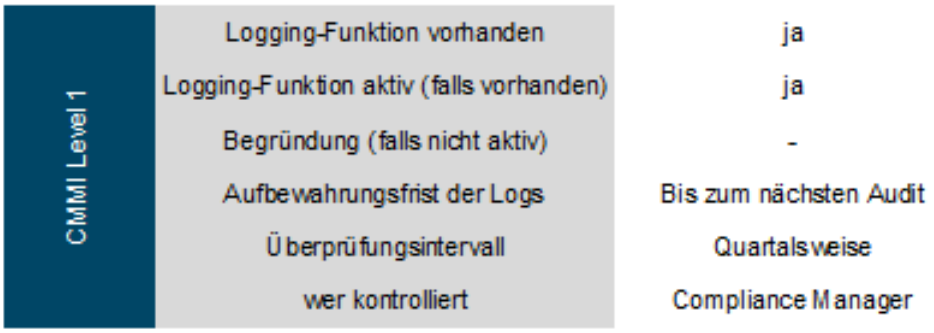


Abbildung 3.3: Konzept für Regel 3

3.3.4 Regel 4

Die Regel 4 befasst sich mit der Anmeldung bei dem System. Hierzu wurde ein Fragenkatalog erstellt. Dieser beinhaltet wie sich angemeldet werden kann mit den Antwortmöglichkeiten: Benutzername, Benutzername und Passwort, PKI[1] und Token[2]. Die Mindestanforderung bei dieser Frage ist Benutzername und Passwort. PKI und Token sind stärker authentifizierende Verfahren, d.h. es wird mindestens eine Zwei-Faktor-Authentifizierung benötigt, z.B. im Falle von PKI, dass man die PKI Karte hat, den PIN dazu kennt und das entsprechende Zertifikat auf der PKI-Karte enthalten ist [IM04]. Es wird weiterhin abgefragt ob diese Accounts mehrheitlich personalisiert sind und ob Built-In-Accounts, soweit technisch möglich, deaktiviert wurden.

Abbildung 3.4 zeigt den ausgefüllten Fragenkatalog für ITP Panorama.

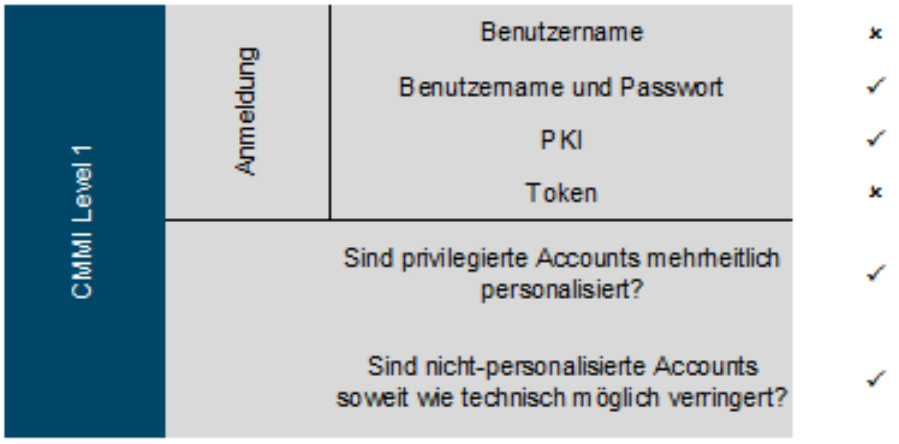


Abbildung 3.4: Konzept für Regel 4

[1]PKI: Publik-Key-Infrastruktur bezeichnet ein System für digitale Zertifikate. Diese können zum Beispiel für Anmeldeprozesse genutzt werden.

[2]Token oder auch Key-Token: bezeichnet ein Verfahren zur Identifikation von Benutzern. Dabei wird bei einem Key-Token, jede Minute ein neues Passwort generiert.

3.3.5 Regel 5

Die Regel 5 befasst sich mit einem Review-Prozess für privilegierte Accounts. Um das CMMI-Level 1 zu erreichen, wurde dafür ein Fragenkatalog entwickelt. Zu den Fragen gehört, ob ein Review-Prozess existiert. Falls dies nicht der Fall ist, muss man es begründen. Falls ein Review-Prozess existiert, muss man beantworten, ob dabei auf die Validität, Aktualität der Accounts eingegangen wird und ob dabei inaktive Accounts deaktiviert werden. Zum Schluss wird gefragt ob Accounts die länger als 90 Tage inaktiv werden, vom System deaktiviert werden. Durch die Dokumentation in dem Konzept wird die letzte Regel automatisch miterfüllt.

Die Mindestanforderungen sind dabei, dass ein Review-Prozess existiert, dieser die privilegierten Accounts auf Validität und Aktualität überprüft und inaktive Accounts deaktiviert werden. Es müssen privilegierte Accounts, die länger als 90 Tage inaktiv waren, deaktiviert werden.

Abbildung 3.5 zeigt den ausgefüllten Fragenkatalog, nach der Verbesserung von ITP Panorama.

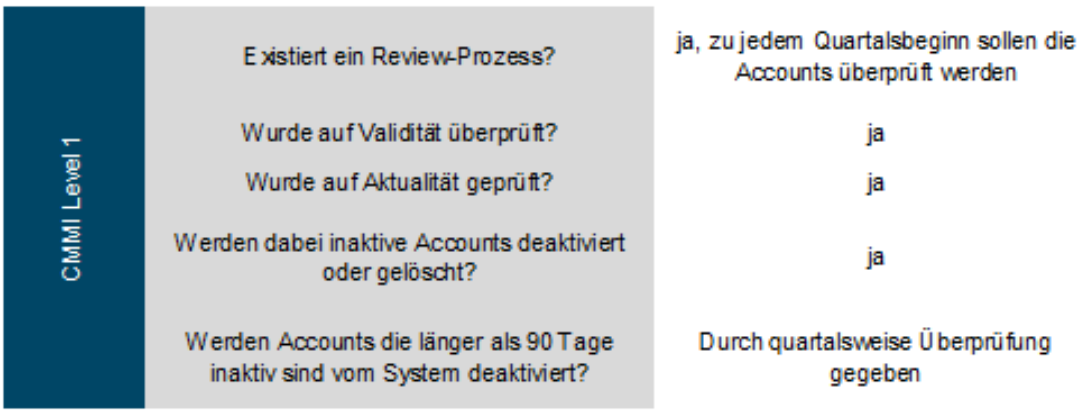


Abbildung 3.5: Konzept für Regel 5

3.3.6 Regel 6

Regel 6 befasst sich mit der Funktionstrennung von privilegierten Accounts. Dafür wurden 8 Rollen gesucht und ausgewählt, mit denen man Systeme darstellen kann. Diese Rollen wurden aufgrund von Erfahrungen mit anderen Systemen ausgesucht. Im nachfolgenden werden diese Rollen genannt und beschrieben. Dabei sind einige Rollen, z.B. Service Owner [nach KB12] vorhanden und andere wurden neu geschaffen, z.B. Administrator.

Lifecycle Owner

- Der Lifecycle Owner ist der Applikationsverantwortliche der Angebotsseite und ist für seine Applikationen und deren Details zur Informations- und Applikationsarchitektur zuständig.

Service Owner

- Der Service Owner ist verantwortlich für die Erbringung eines Infrastruktur-Services im Rahmen der vereinbarten Service Levels.
- Er tritt als Verhandlungspartner des Service Level Managers auf, wenn es darum geht, Operational Level Agreements (Vereinbarungen auf Betriebsebene) zu vereinbaren.
- Häufig handelt es sich bei dem Serviceverantwortlichen um eine Führungskraft, die ein Team technischer Spezialisten oder einen internen Support-Bereich leitet.

Compliance Manager

- Der Compliance Manager trägt die Verantwortung dafür, dass die gültigen Standards und Richtlinien befolgt werden. Er sorgt vor allem für die Einhaltung unternehmensspezifisch vorgegebener Verfahren und externer gesetzlicher Vorschriften.

Administrator

- Ein Administrator ist ein Benutzer, der über zusätzliche spezielle Berechtigungen verfügt. Diese Berechtigungen stellen ihm Werkzeuge zur Verfügung, mit denen bestimmte Verwaltungsaufgaben eines IT-Systems, einer Applikation, einer Schnittstelle oder eines Betriebssystems vorgenommen werden können. Die Möglichkeiten reichen über die eines Benutzers bei der täglichen Arbeit hinaus. Die Definition ist losgelöst von jeglichem IT-System, dem Netzwerk oder den Applikationsbeschreibungen. Die Rolle „Administrator" und die Anwendung der damit verbundenen Berechtigungen ist unabhängig von Sicherheitszonen, Netzwerksegmenten, der eingesetzten Technik und von den Netzwerk-Sites (wie z.B. Intranet oder Internet).

Deployer

- Ein Deployer ist ein Benutzer, der Anwendungen konfigurieren und verändern kann.

Problem Analyst

- Der Problem Analyst ist für die operative Umsetzung aller Prozessschritte nach Vorgabe des Problem Managers verantwortlich.
- Aufgabe sind z.B.: Auswertung von Systeminformationen, Problemanalyse mit dem kurzfristigen Ziel, einen Workaround zu erarbeiten

Supporter

- Der Applikationsmanager ist der Applikationsverantwortliche der Angebotsseite und ist für seine Applikationen und deren Details zur Informations- und Applikationsarchitektur zuständig.
- Bei Bedarf wird er Unterstützung von Herstellern (3rd Level Support) anfordern.
- Ziel ist die schnellstmögliche Wiederherstellung des definierten Betriebszustands eines Service.

Developer

- Der Anwendungsentwickler ist dafür verantwortlich, Anwendungen und Systeme bereitzustellen, die die erforderliche Funktionalität für die IT-Services gewährleisten.
- Dies umfasst die Entwicklung und die Instandhaltung von kundenspezifischen Anwendungen ebenso, wie die Anpassung externer Standardsoftware.

Aus diesen Rollen und den damit verbundenen Arbeiten wurde eine Funktionstrennungsmatrix erstellt. Diese soll aufzeigen, welche Rollen miteinander kompatibel sind, also welche Rollen mehrfach von nur einer Person ausgeführt werden könnten. In Abbildung 3.6 ist erkennbar, dass jede Rolle mit sich selbst kompatibel ist und somit jede Rolle für sich betrachtet, ausführbar ist. Die Rolle des Compliance Managers ist nur mit sich selbst kompatibel, da er die Einhaltung von Standards überwachen soll.

	Service Owner	Lifecycle Owner	Compliance Manager	Administrator	Deployer	Problem Analyst	Supporter	Developer
Service Owner	✓							
Lifecycle Owner	✗	✓						
Compliance Manager	✗	✗	✓					
Administrator	✓	✓	✗	✓				
Deployer	✓	✓	✗	✗	✓			
Problem Analyst	✓	✓	✗	✗	✗	✓		
Supporter	✓	✓	✗	✗	✗	✓	✓	
Developer	✓	✓	✗	✗	✗	✗	✗	✓

Abbildung 3.6: Funktionstrennungsmatrix

Nachdem die Grundlagen für die Funktionstrennung geschaffen wurde, wurde eine Tabelle entwickelt, die für das CMMI-Level 1 auszufüllen ist. Dabei werden alle Login-Namen automatisch übernommen und man muss diesem die entsprechende Rolle oder Rollen im System zuweisen. Aus diesen Rollen ist erkennbar, welche Tätigkeiten ausgeführt werden, z.B. ist die Tätigkeit des Compliance Managers, eine prüfende und die eines Administrators, eine operative. Weiterhin werden die Aufgaben des Users eingetragen, dabei dient diese Rollenbeschreibung als Referenz. Es müssen die benötigten Rechte eingetragen werden, z.B. bei dem Compliance Manager, dass er lesenden Zugriff auf das System hat, um zu prüfen ob Standards eingehalten werden, oder dass der Administrator schreibende Rechte für das System hat. Zum Schluss muss noch ausgefüllt werden, ob ein Rollenkonflikt vorhanden ist. Diese muss anhand der Funktionstrennungsmatrix überprüft werden. Weiterhin muss noch überprüft werden, ob ein Unterstellungsverhältnis existiert.

Aus datenschutzrechtlichen Gründen wird in dieser Arbeit nur das Konzept abgebildet und nicht die für ITP Panorama ausgefüllte Tabelle.

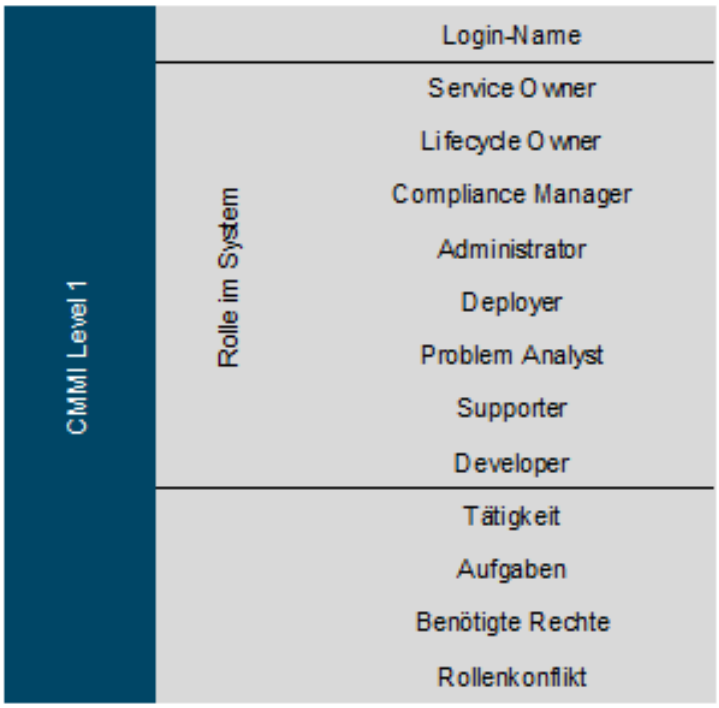


Abbildung 3.7: Konzept für Regel 6

3.3.7 Regel 7

Regel 7 befasst sich mit den Built-In-Accounts. Dabei wird ein Teil der zu erfüllende Maßnahmen, die Dokumentation der Built-In Accounts, schon mit Regel 2 erfüllt. Für die weiteren Maßnahmen wurde ein Fragenkatalog entwickelt. Dabei wird auf die Sicherheitsanforderungen bei den Built-In-Accounts eingegangen, sowie ob und durch wen die Sicherheitsanforderungen überprüft werden. Falls sie nicht überprüft werden, muss dieses begründet werden.

Die Mindestanforderungen sind, dass die Sicherheitsanforderungen dokumentiert werden und diese Sicherheitsanforderungen mindestens stichprobeartig überprüft werden.

Abbildung 3.8 zeigt den ausgefüllten Fragenkatalog, nach der Verbesserung von ITP Panorama.

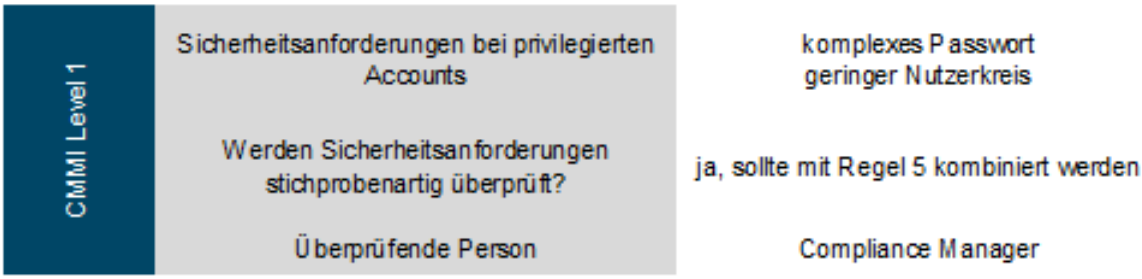


Abbildung 3.8: Konzept für Regel 7

3.3.8 Regel 8

Regel 8 befasst sich mit den privilegierten Accounts, die für eine Fernwartung eingerichtet sind. Dabei werden aus Regel 2 alle Login-Namen automatisch übernommen und es muss ausgefüllt werden, ob eine Fernwartung möglich ist und, falls sie möglich ist, muss eine Begründung eingetragen werden.

Aus datenschutzrechtlichen Gründen, wird in dieser Arbeit nur das Konzept abgebildet und nicht die für ITP Panorama ausgefüllte Tabelle. Angemerkt sei hierbei, dass kein Nutzer einen Fernwartungszugriff hat.

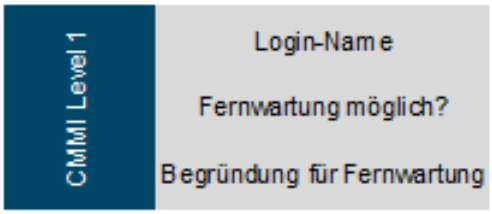


Abbildung 3.9: Konzept für Regel 8

3.3.9 Regel 9

Regel 9 befasst sich mit einem Notfall-User-Prozess. Hierbei wird die Definition eines Notfalls und der Notfall-User-Prozess dokumentiert.

Aus datenschutzrechtlichen Gründen wird hier eine verkürzte Fassung des Notfallplans dargestellt. Die Definition stammt von [BSI008].

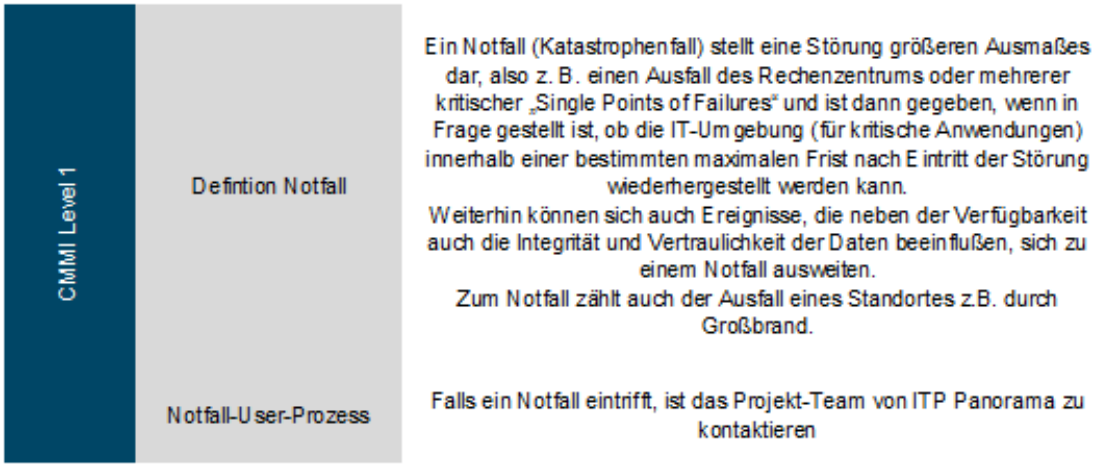


Abbildung 3.10: Konzept für Regel 9

4. Zusammenfassung und Ausblick

In diesem Kapitel sollen die Ergebnisse der Auditierung von ITP Panorama dargestellt, sowie ein Ausblick gegeben werden.

4.1 Auditierung ITP Panorama

Das System ITP Panorama wurde im Kontext von DIALOGplus nach Verbesserung des Systems auditiert.

Durch die direkte Arbeit mit dem Regelwerk, wurden dabei alle Punkte erfüllt und somit CMMI-Level 1 erreicht. Bei der Auditierung wurde auch bestätigt, dass Regel 1, welche die allgemeinen Randbedingungen betrachtet, nicht auditiert wird und als gegeben angenommen wird. Es wurde auch herausgestellt, dass ein Notfall-Userprozess in diesem Fall nicht notwendig wäre, da es erstens kein geschäftskritisches System ist und zweitens bei Verlust der entsprechende Server, die Daten von den Ursprungssystemen gerettet werden können; d.h. wenn der ITP Panorama Server verloren geht, kann man dafür einen Ersatz schaffen und die entsprechenden Quellsourcen wieder neu einspielen.

Da das System wenige privilegierte Accounts hat, wurde vom Auditor vorgeschlagen für Regel 5, dem Review-Prozess, auf halbjährlich zu verlängern. Dieses wurde aber abgelehnt, da man bei quartalsweiser Überprüfung gleichzeitig den Punkt der 90-tägigen Überprüfung der inaktiven Accounts bearbeitet.

Es wurde als positiv angemerkt, dass mit diesem Konzept die Dokumentation erreicht wird. Es muss aber überlegt werden, wie dieses Dokument abgelegt wird, so dass nicht jeder Zugriff darauf hat und wie man eventuelle Veränderungen erkennbar macht. Dazu wurde schon eine Ablage mit Versionsverwaltung, wie sie z.B. der eRoom von EMC Corporation [1] bietet, in Betracht gezogen, da man so erkennt wer die letzte Veränderung getan hat. Aber es kann nicht einfach herausgefiltert werden, was verändert wurde. Ein weiterer Vorschlag ist die Entwicklung eines entsprechenden Makros.

[1] http://www.eroom.net/ [IQ6]

Es wurde auch bestätigt, dass man CMMI-Level 1 mit dem Konzept erreicht, solange man die Mindestanforderungen beachtet.

4.2 Ausblick

Der Anfang des Ausblicks beschäftigt sich mit dem Konzept. Dieses benötigt eine Freigabe, sodass weitere Systeme damit untersucht werden können. Außerdem muss geklärt werden, welche Personen darauf Zugriff bekommen, sowie wie die Versionshistorie gestaltet werden soll.

Nachdem man alle Systeme untersucht und mit CMMI-Level 1 bewertet wurden, kann man das Konzept zum Erreichen von CMMI-Level 2 erweitern. Nachfolgend werden Maßnahmen für CMMI-Level 2 aufgezeigt.

Regel 2

- Auflistung der privilegierten Accounts sind standardisiert und an einem definierten Ort hinterlegt
- Der Prozess wird für die Accounts mit administrativen und privilegierten Rechten für alle Stufen, vom Einrichten im System bis zur Löschung aus dem System, detailliert und nachvollziehbar beschrieben
- Beim Ausscheiden von Benutzern mit administrativen, bzw. privilegierten Rechten werden die Accounts innerhalb von maximal drei Tagen im System gesperrt
- Für alle Stufen der Prozesse sind Verantwortliche benannt, das Minimal-Prinzip und das Vier-Augen-Prinzip werden durchgehend angewendet

Regel 3

- Alle eingesetzten IT-Systeme der Konzernstelle, für die die Kriterien aus dem aktuellen ISSO-IT-Sicherheitsregelwerks zutreffen (d. h. alle IT-Systeme, die Daten der Klassifikation „vertraulich“ oder höher enthalten), werden so konfiguriert, dass Sessions mit administrativen und privilegierten Rechten geloggt werden
- Für den Prozess der Protokollierung der Aktivitäten von Systemadministratoren sind Verantwortliche benannt.
- Die Log-Dateien können nicht von den Administratoren verändert oder gelöscht werden

Regel 4

- Alle Accounts mit administrativen und privilegierten Rechten verwenden bei der Anmeldung an allen IT-Systemen, die geheime bzw. personenbezogene Daten enthalten, eine starke Authentisierung

- Soweit noch nicht-personalisierte Accounts für den Zugriff auf diese Systeme eingesetzt werden müssen, sind die Benutzergruppen so klein wie möglich zu halten. Die Arbeit mit diesen Accounts muss vollständig protokolliert und begründet werden
- Die Verantwortung für die Benutzer-Authentifikationsprozesse wird eindeutig einer Organisationseinheit zugeordnet

Regel 5

- Für alle IT-Systeme wurde eine Initiale Bereinigung der Accounts mit administrativen bzw. privilegierten Rechten durchgeführt
- Administrative Accounts die für einen Zeitraum von 30 Tagen nicht mehr genutzt wurden, werden in den IT-Systemen deaktiviert
- Alle Ergebnisse und die sich daraus ergebenen Handlungen bezüglich der administrativen Accounts und deren Rechte werden einheitlich dokumentiert und die Dokumentationsunterlagen werden sicher aufbewahrt

Regel 6

- Administratoren haben keine administrativen Berechtigungen in aufeinander aufbauenden bzw. voneinander abhängigen Systemen
- Die Umsetzung der Lösungen zur Funktionstrennung wird in der gesamten Organisationseinheit/Konzernstelle nach einem einheitlichen, abgestimmten Prozess durchgeführt und dokumentiert
- Konflikte in Bezug auf Funktionstrennung/Rechteüberschneidungen werden durch die eingerichteten Prozesse innerhalb der OE/Konzernstelle beim Einrichten von administrativen Accounts in den IT-Systemen automatisch erkannt und behoben

Regel 7

- Die zusätzlichen Sicherheitsanforderungen für besondere Accounts mit privilegierten Rechten werden für die gesamte Konzernstelle vereinheitlicht
- Es wird ein System zum Application Password Management eingeführt
- Es wird ein System zur automatisierten Änderung von Passwörtern dieser Accounts nach jeder Benutzung eingeführt

Regel 8

- Für die Accounts mit administrativen bzw. privilegierten Rechten, die Fernwartung durchführen, werden hohe Sicherheitsanforderungen angewendet, wie starke Authentifizierung

Regel 9

- Mit der Dokumentation vom Notfall-Userprozess in dem Konzept wird CMMI-Level 2 erreicht

Nachdem man CMMI-Level 2 für alle Systeme erreicht hat, wird ein Tool für die Verwaltung von privilegierten Accounts eingeführt, wie z.B. Cyber Arks Privileged Identity Management-Suite [2], um die Voraussetzungen für CMMI-Level 3 zu schaffen. Abbildung 4.1 zeigt die grundlegenden Eigenschaften eines solchen Systems. Es soll ein zentrales System sein, mit dem sich auf andere Systeme angemeldet werden kann. Bei dieser Anmeldung wird überprüft, ob der Anwender Zugriff auf das System hat und generiert gegebenenfalls ein Einmalkennwort. Außerdem soll das Tool zur Protokollierung dienen.

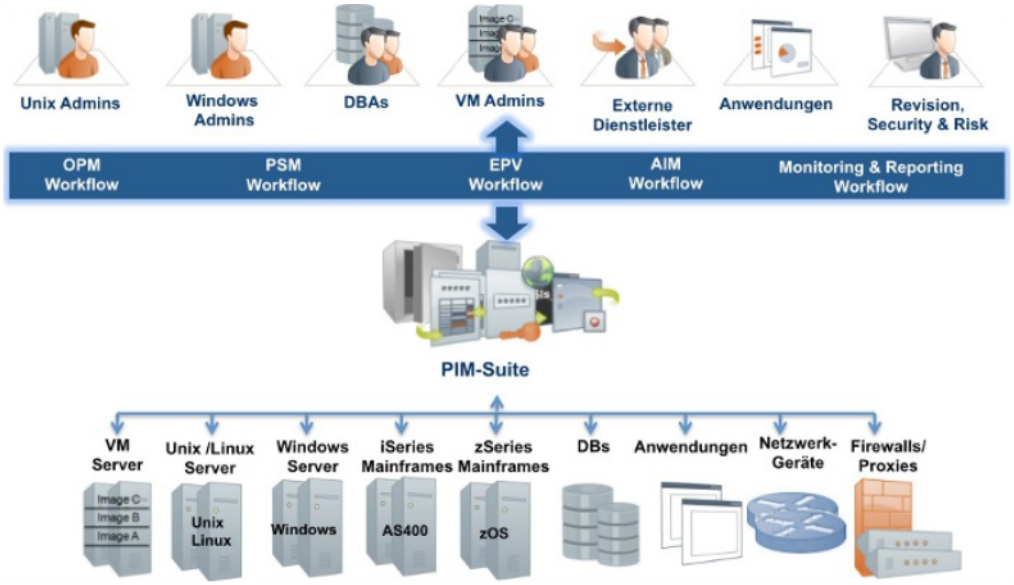


Abbildung 4.1: Cyber-Ark aus [SM13]

4.3 Fazit

Ein Ziel dieser Arbeit war es, das Regelwerk vorzustellen und dieses am Beispiel von ITP Panorama anzuwenden. Dies geschah in Abschnitt 2.4 und Abschnitt 3.1. Es folgte das Ziel der Konzeption für weitere Systeme in Abschnitt 3.3. Das Ziel der Erreichung von CMMI-Level 1 wurde zum einem in Abschnitt 3.2 und in Abschnitt 4.1 bestätigt.

Mit Hilfe dieser Arbeit wurden Grundlagen für das weitere Vorgehen des Projektes IT Security Programm 4.4 geschaffen. Dabei wurde nicht nur ein Konzept erstellt, sondern im weiteren Verlauf der Arbeit auch positiv auditiert.

Im Verlauf der Arbeit hat sich herausgestellt, dass die Anpassung des Tools an das Regelwerk sehr aufwändig ist. Hier sollte man immer vorher eine Kosten-Nutzen-Analyse machen, da z.B. ein detaillierter Notfall-User-Prozess am Beispiel von ITP

[2] http:www.cyber-ark.com/de[IQ7]

Panorama viel Aufwand benötigt und im Audit herausgestellt wurde, dass bei diesem System, unter dem Umstand der Datenrekonstruktion, eine Dokumentation der verantwortlichen Person reicht. Dabei kam öfters die Frage auf, lohnt sich die Anwendung des Regelwerkes an kleineren Systemen mit wenigen privilegierten Nutzern? Am Anfang der Arbeit war die Sicht des Autors, dass ein vollständiges Betriebshandbuch hinreichen würde, da dort die meisten Daten erfasst wurden und, falls weitere Fragen bestehen, man dort die zuständigen Personen benennt. Diese Sichtweise hat sich mit dem Konzept und der Auditierung verändert. Das Konzept schafft eine gemeinsame Grundlage für CMMI-Level 1 und die Auditierung hat aufgezeigt, dass man die weiteren CMMI-Level betrachten muss.

Es hat sich herausgestellt, dass der Begriff *privilegierte Accounts* nicht eindeutig ist und je nach Betrachtungsweise unterschiedliche Accounts dazu zählen. Zum Beispiel betrachtet man nur ITP Panorama ergeben sich 2 privilegierte Accounts aber wenn man die einzelnen Hypercubes betrachtet, ergeben sich mehr privilegierte Accounts, da jeder Nutzer, der Zugriff auf einen Hypercube hat, privilegiert ist den Source-Code zu analysieren und somit Einsichten in ein System hat.

4.4 Zusammenfassung

Die Arbeit gab am Anfang eine Einleitung und Motivation zum Thema Privileged Identity Mangement. Darauffolgend wurden die Grundlagen zur weiteren Bearbeitung geschaffen, wie die Vorstellung von CMMI, ITIL und dem Regelwerk. Es folgte die Ist-Analyse mit der Erkenntnis von Defiziten bei ITP Panorama, sowie Korrekturvorschläge. Danach wurde ein Konzept für weitere Systeme vorgestellt. Anschließend wurde eine Auswertung des Konzepts mit Hilfe eines Audits gegeben. Zum Schluss folgten ein Ausblick, sowie ein Fazit.

A. Anhang

A.1 FTD Bericht [IQ2]

25.08.2011, 04:00

Cyberkriminalität: Enorme Sicherheitslücken bei VW

Eine interne Untersuchung hat die Gefahr eines Hackerangriffs auf den Autohersteller schonungslos aufgedeckt. Volkswagen schweigt offiziell zu den Risiken - doch Insider verweisen auf die veraltete IT des Wolfsburger Konzerns. von Margret Hucko und Annika Graf, Hamburg

Bei Volkswagen gibt es gravierende Sicherheitslücken im konzerneigenen Computersystem. Nach FTD-Informationen hat eine interne Untersuchung von Experten der Unternehmensberatung PricewaterhouseCoopers offengelegt, dass Europas größter Autohersteller nur schlecht gegen mögliche Hackerangriffe abgesichert ist - und sensible Firmengeheimnisse zu leicht abgefischt werden können.

“VW ist bereits dabei, diese Löcher zu stopfen”, sagte ein Insider. Der Autobauer wolle in den kommenden Jahren einen dreistelligen Millionenbetrag in eine besser geschützte Informationstechnologie investieren, hieß es. Der mächtige Aufsichtsratsvorsitzende Ferdinand Piëch habe die IT-Sicherheit zur Chefsache erklärt. Bislang soll es indes noch keinen Übergriff auf das Datensystem der Wolfsburger gegeben haben.

Die groß angelegte Hackerattacke auf den japanischen Elektronikhersteller Sony im April hatte gezeigt, wie angreifbar große Konzerne durch die zunehmende Vernetzung mit dem Internet geworden sind. Weltweit werden Unternehmen immer häufiger Opfer von gezielten Attacken, die oftmals auch Wirtschaftsspionage vermuten lassen. Teilweise verwenden Hacker mehrere Monate darauf, Sicherheitslücken auszuspähen.

Volkswagen weiß offenbar schon länger von den Schwachstellen im eigenen System. Seit PricewaterhouseCoopers Anfang des Jahres die Ergebnisse der Untersuchung vorgestellt hat, ist das Ausmaß der Probleme auch einem größeren Kreis von Managern bekannt. Vorstand und Aufsichtsrat wurden darüber informiert, wie groß die Gefahr eines Hackerangriffs ist.

Inzwischen muss deswegen Volkswagens IT-Chef Klaus Hardy Mühleck um seinen Job bangen. Ihm wird vorgeworfen, zu spät auf die dramatischen Erkenntnisse reagiert zu haben. Mühleck gehört zu den wichtigsten IT-Managern in Deutschland. In Wolfsburg hat er den Rang eines Generalbevollmächtigten und berichtet direkt an VW-Chef Martin Winterkorn.

Ein Angriff auf das IT-System des Konzerns könnte schwerwiegende Folgen haben. Die Computer von Volkswagen sind nicht nur zwischen den einzelnen Konzernmarken wie Audi, Seat oder Skoda vernetzt, sondern auch zwischen den insgesamt 22 Ländern, in denen das Unternehmen produziert.

Hacker könnten beispielsweise dafür sorgen, dass wichtige Bauteile am Band fehlen - und so die ganze Fertigung gefährden. Noch größer könnte der Schaden sein, wenn Kriminelle Betriebsgeheimnisse wie technische Details künftiger Modelle stehlen.

Insider sprachen von einem Investitionsstau beim Computersystem von Volkswagen. Veraltete Technik und nicht ausreichend gesicherte Programme seien ein häufiges Problem in deutschen Unternehmen, sagte Timo Kob, Vorstand der IT-Sicherheitsberatung Hisolutions.

Ein VW-Sprecher wollte sich am Mittwoch zu Einzelheiten nicht äußern. Generell arbeite der Konzern mit IT-Standards, die “in einem laufenden Prozess ständig auf den höchsten Stand gebracht werden”.

VW-Patriarch Piëch gilt als sehr sicherheitsbewusst. Der ehemalige Chefermittler im Reemtsma-Entführungsfall, Dieter Langendörfer, lange Sicherheitschef des Konzerns, wurde anschließend sein Leibwächter.

B. Literaturverzeichnis

BF11 Dominik Brodowski and Felix C. Freiling, Cyberkriminaltität Computerstrafrecht und die digitale Schattenwirtschaft, Buch, ACM Press/Addison-Wesley, Seite 11, 2011

BSI08 Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standard 100-1 Managementsysteme für Informationssicherheit (ISMS) Godesberger Allee 185-189, 53175 Bonn, S. 11, 12, 2008 (Version 1.5) www.bsi.bund.de/gshb

BSI8 Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standard 100-4, Notfallmanagement Postfach 20 03 63 , 53175 Bonn, S. 5, 2008 (Version 1) www.bsi.bund.de/gshb

BSI008 Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Profile, Referat 114 -IT-Sicherheitsmanagement und IT-Schutz, Postfach 20 03 63 , 53175 Bonn, S. 6, 7, 2008 www.bsi.bund.de/gshb

CKS09 Chrissis, Mary Beth, Konrad, Mike und Shrum, Sandy. CMMI - Richtlinien für Prozess - Integration und Produkt-Verbesserung. s.l. : Addison-Wesley, 2009. S. 761, 780, 59, 60 ISBN: 978-3-8273-2784-0

IM04 Walther, Horst. Identity Management. HMD Praxis der Wirtschaftsinformatik 238 (2004): 92-100

ITS11 Dr. Sebastian Steffens, Management und Risikomanagement für privilegierte Accounts, Vom Umgang mit den ÄllrechtigenÏn: IT Sicherheit, 06/2011, S. 52-53

IQ1 Norton by Symantec, 2012 Norton Cybercrime Report http://www.norton.com/2012cybercrimereport, zuletzt aufgerufen: 05.06.2013

IQ2 Aus der Financial Times Deutschland vom 25.08.2011, FTD Cyberkriminalität Enorme Sicherheitslücken bei VW http://www.ftd.de/unternehmen/industrie/:cyberkriminalitaet-enorme-sicherheitsluecken-bei-vw/60095257.html, zuletzt aufgerufen: 12.06.2013

IQ3 ITP-Panorama Inc. http://www.itp-panorama.com, zuletzt aufgerufen: 02.07.2013

IQ4 ITIL-Wiki, Best Management Practise, http://www.wiki-itil.de/Rollen in ITIL V3, zuletzt aufgerufen: 15.06.2013

IQ5 Köhler, Stefan, Priviledged Identity Management zur Kontrolle kritischer Benutzerkonten, vom 06.12.2010 http://www.searchsecurity.de/themenbereiche/identity-und-access-management/user-management-und-provisioning/articles/294910/, zuletzt aufgerufen: 06.06.2013

IQ6 EMC Documentum eRoom.net, http://www.eroom.net, zuletzt aufgerufen: 13.07.2013

IQ7 Cyber-Ark, Cyber-Ark Software
http:www.cyber-ark.com/de,
zuletzt aufgerufen: 14.07.2013

IQ8 Keller, Anne-Kathrin, Pleite der Woche: Zeitungssterben die Zweite.,
http://www.absatzwirtschaft.de/content/communication/news/ftd-pleite-taz-kreativ-deutsche-bank-ohne-slogan-und-hollywoodglamour-beim-bambi;78606
zuletzt aufgerufen: 22.07.2013

IQ9 Regierungskommission, Deutscher Corporate Governance - Kodex
http://www.corporate-governance-code.de/ger/kodex/4.html
zuletzt aufgerufen: 10.07.2013

KB12 Michael Kresse and Markus Bause, ITIL® Alles was man wissen muss Edition 2011, SERVIEW GmbH, 2.Auflage 2012, S. 80, 91, 106, 109, 134, 140, 184, 215, 220, 226, 227, 228
ISBN: 978-3-9813151-6-5

SM13 http://www.securitymanager.de/magazin/privileged identity management fluch oder segen.html, zuletzt aufgerufen: 15.07.2013

VW13 Marc Gellenbeck, Leitfaden Privileged Identity Management INTERN, 2013 (V1.1)s

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

Magdeburg, den 02.08.2013