Prüfstelle
Organismo di valutazione
Organn de valutazion

Berechtigungs- und Zugriffskonzept in SAP

Erhebung im Sinne von Artikel 24, Absatz 1, Buchstabe a) des LG Nr. 10/1992 in geltender Fassung

Südtiroler Landtag
Consiglio della Provincia autonoma di Bolzano
Cunsëi dla Provinzia autonoma de Bulsan

PRÜFERIN	Eva Maria Kofler
PRÜFER	Martin Steinmann

PRÜFSTELLE
ORGANISMO DI VALUTAZIONE

39100 Bozen | Freiheitsstraße 66
39100 Bolzano | Corso Libertà, 66

Tel. 0471 402 212 | Fax 0471 260 114
pruefstelle@landtag-bz.org | organismodivalutazione@consiglio-bz.org
www.landtag-bz.org/de/pruefstelle.asp
www.consiglio-bz.org/it/organismo-di-valutazione.asp
PEC: pruefstelle.organismovalutazione@pec.prov-bz.org

August 2020

INHALT

I. Normativer Kontext, Begründung und Ziel der Erhebung

Im Sinne von Artikel 24, Absatz 1, Buchstabe a) des LG Nr. 10/1992 in geltender Fassung überwacht die Prüfstelle die Funktionsweise des Systems der internen Kontrollen (im folgenden IKS genannt) innerhalb der Landesverwaltung. Das IKS soll sicherstellen, dass das Erreichen der Organisationsziele nicht durch interne und externe Risiken gefährdet wird.

IKS-Prüfungen sind besonders in jenen Bereichen sinnvoll, die mit relevantem Risiko behaftet sind. Die Relevanz des Risikos ist einerseits am potenziellen monetären Schadensausmaß, andererseits aber auch an der potenziellen Beeinträchtigung der Funktionsfähigkeit der Aufgabenwahrnehmung zu messen. Zunehmend gewinnen die Risiken im Bereich der Informationstechnik an Bedeutung, etwa im Bereich der Privacy, Daten- Informationssicherheit und Integrität. Den Berechtigungs- und Zugriffkonzepten zu den IT-Systemen kommt daher eine zentrale Rolle in der Eindämmung und Verhinderung dieser Risken zu.

Im Jahre 2015 hat die Prüfstelle eine allgemeine IKS-Prüfung und in den folgenden Jahren spezifische Prüfungen in ausgewählten Bereichen durchgeführt. Im Rahmen des Jahresarbeitsprogramms 2020 und im Sinne einer Diversifizierung der zu prüfenden Bereiche, war es Ziel der gegenständlichen Prüfung, die Funktionsweise des IKS auf Ebene der SAP-Anwendung in der Südtiroler Landesverwaltung zu erheben. Die Erhebung beruht auf dem implementierten Berechtigungs- und Zugriffskonzept, welches Aspekte eines funktionierenden IKS abdecken sollte.

II. Methodischer Ansatz und Umfang

Das Vorantreiben einer zunehmenden digitalen Verwaltung gehört seit Jahren mit zu einem der zentralen Handlungsfelder in der Südtiroler Landesverwaltung[1]. Zusätzlich verstärken die Erfahrungen aus der COVID-19 Pandemie die Entwicklung zu einer digitalen Verwaltung. Eine digitale Verwaltung bringt zahlreiche Vorteile, sei es für die Bürger und Unternehmen als auch für die öffentliche Verwaltung selbst. Verbunden sind damit auch Risiken (Privacy, Amtsgeheimnis), die analysiert und berücksichtigt werden müssen.

In diesem Rahmen spielen die IT-Systeme eine zentrale Rolle. Ein Informationssystem ist laut ISACA Deutschland e.V. (Information Systems Audit and Control Association) ein soziotechnisches System, das aus technischen (Hardware, Software, Daten), organisatorischen (Rollen und Berechtigungen) und fachlichen Komponenten (Geschäftsprozesse) besteht und verschiedene zu schützende Werte unterschiedlicher Komplexität beinhaltet[2]. Laut ISACA, welche als eine weltweite Referenz im Bereich der IT-Governance und Sicherheit gilt[3], sollen mit Bezug auf die IT folgende Ziele verfolgt werden:

- Vermeidung von Verstößen gegen Gesetze und andere Regelungen
- Langfristiger Schutz des Unternehmens vor (monetären und nicht monetären) Schäden aus und für die IT
- Erhaltung der Leistungsfähigkeit der IT und damit der Geschäftsprozesse und Geschäftsmodelle des Unternehmens
- Gewährleistung des internen Kontrollsystems in der IT.

Die Information stellt sowohl für die öffentliche Verwaltung als auch für Organisationen der Privatwirtschaft einen wichtigen Wert dar[4]. Information kann dabei in unterschiedlicher Form existieren

[1] Südtirol digital 2020: https://issuu.com/landsuedtirol-provinciabolzano/docs/sudtirol_digital_2020_de_neu
[2] https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_ii_2016_gesamt_screen.pdf
[3] https://www.agendadigitale.eu/infrastrutture/centri-di-elaborazione-dati-ced-cose-come-funziona-costi-e-normativa/
[4] Österreichisches Sicherheitshandbuch: https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf

– elektronisch gespeichert oder übertragen, geschrieben, als Bild oder in gesprochener Form. Diese Beschreibung geht mit der im Artikel 24 des LG Nr. 17 vom 23. Oktober 1993 (Regelung des Verwaltungsverfahrens) enthaltenen Definition von Verwaltungsunterlage konform.
Die Tatsache, dass immer mehr Bereiche des täglichen Lebens ohne den Einsatz von informationstechnischen Systemen heute nicht mehr funktionsfähig sind, rückt die Frage nach der Sicherheit der Informationen und der Informationstechnologie zunehmend in den Brennpunkt des Interesses[5].
Es gilt daher die in IT-Systemen in großer Anzahl gespeicherten Informationen sachgemäß zu verwalten.
Dieser herausragenden Bedeutung zum Schutz von Informationen hat der italienische Gesetzgeber, neben strafrechtlichen Bestimmungen (Artikel 615ter StGB), auch durch eine Reihe von Bestimmungen im Bereich Privacy Rechnung getragen. So hat die Datenschutzbehörde (Garante per la protezione dei dati personali) etwa spezielle Bestimmungen zu den Administratoren solcher Systeme erlassen (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema)[6]. Den Administratoren kommt daher eine zentrale Rolle zu, da sie den Überblick und den Zugang zu sämtlichen Informationen haben können. Wesentlich sind daher die Verfahren zur geordneten und dokumentierten Erteilung von Berechtigungen, welche die Zugriffsmöglichkeiten steuern. Diese sollen über die gesamte Lebensdauer (life cycle) des Zugriffsrechtes wirken, also von der erstmaligen Einrichtung neuer BenutzerInnen bis zur Entfernung, wenn kein Zugriff mehr benötigt wird. Besonders relevant ist dabei die Kontrolle über privilegierte Zugriffsrechte (Superuser), da damit Systemkontrollen außer Kraft gesetzt werden könnten[7].

Bei der Wahrnehmung der gegenständlichen Bewertung orientiert sich die Prüfstelle auch an folgenden IKS-relevanten Aspekten:

- **Transparenz-Prinzip, Grundsatz der Nachvollziehbarkeit:** klare, detaillierte und transparente Regelung der Arbeitsabläufe, Unterlagen und Abläufe sind nachvollziehbar zu dokumentieren,
- **Kontrollautomatik und Vier-Augen-Prinzip:** systematischer Einbau von Kontrollen im Arbeitsablauf, wobei diese Kontrollen IT-gestützt oder durch Implementierung von Gegenkontrollen erfolgen können,
- **Prinzip der Funktionstrennung:** keine Allein-Verantwortung für den gesamten Prozess; konsequente Trennung von entscheidender, ausführender und kontrollierender Funktion,
- **Aufgaben- und verantwortungsadäquate Informationsbereitstellung:** (Prinzip der Mindestinformation): Bereitstellung jener Informationen an Management und Mitarbeiter, die zur Erfüllung der Aufgaben notwendig sind,
- **Aufgaben- und verantwortungsadäquate Zugangs- und Zugriffsberechtigungen (Prinzip der „minimalen Rechte"):** Zugangs- und Zugriffsberechtigungen (z.B. zu IT-Systemen) müssen adäquat beschränkt sein; Einräumung nur jener Berechtigungen zu sensiblen Daten, die zur Erfüllung der Aufgaben unbedingt erforderlich sind,
- **IKS als kontinuierlicher Prozess:** regelmäßige und systematische Überprüfung des IKS auf seine Funktionsfähigkeit, Wirksamkeit und Aktualität, um sicherzustellen, dass die internen Kontrollen dauerhaft/nachhaltig wirksam sind und bei Änderung der Rahmenbedingungen entsprechend angepasst werden,
- **Grundsatz der Kosten-Nutzen-Abwägung:** der mit Kontrollen verbundene Aufwand bzw. Ressourceneinsatz soll in einem angemessenen Verhältnis zu dem zu vermeidenden Risiko (Schadensausmaß und Eintrittswahrscheinlichkeit) stehen.

Für gegenständliche Erhebung wurde ein Fragenkatalog, basierend auf den oben angeführten IKS - relevanten Aspekten, ausgearbeitet und der Abteilung 9 (Informationstechnik) in einem Gespräch unterbreitet. Dabei ist vereinbart worden, den Fragenkatalog einzig der Abteilung 9 zuzusenden, da

[5] Österreichisches Sicherheitshandbuch: https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf
[6] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499
[7] Österreichisches Sicherheitshandbuch: https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf

diese in Ausübung der Governance über die SIAG ihrerseits die eventuell notwendigen Informationen und Sachverhalte einholen wird.

Um eine Analyse der Ausprägung des internen Kontrollsystems (IKS) des Berechtigungs- und Zugriffskonzeptes in SAP durchführen zu können, erscheint es zunächst zielführend, die SAP-Systemlandschaft in der Landesverwaltung zu erheben. Da ein gut funktionierendes IKS auf organisatorischen Regeln aufbaut, werden die technischen Möglichkeiten und Lösungen, die SAP standardmäßig anbietet, nicht vertieft. Anschließend werden in den darauffolgenden zwei Abschnitten die Ebene der Anwender und der Administratoren analysiert.

III. Sachverhaltsdarstellung

Wie im vorher gehenden Kapitel erläutert, wird die Darstellung des Sachverhalts, auch aufgrund einer besseren Lesbarkeit, in drei Abschnitte unterteilt. Die Ausführungen basieren auf den schriftlichen Antworten und Unterlagen, die von der Abteilung Informationstechnik zur Verfügung gestellt worden sind.

3.1. SAP-Systemlandschaft

In der Südtiroler Landesverwaltung wird bereits seit Jahren die gesamte Finanzgebarung über SAP (Systeme Anwendungen und Produkte in der Datenverarbeitung) abgewickelt[8]. Dazu gehören, neben der klassischen öffentlichen (kameralistischen) Buchhaltung, auch die Vermögensbuchhaltung und die Bilanzbuchhaltung. Demnächst werden auch Teile der Anwendung Human Ressource (HR) für die Mitarbeiterverwaltung zum Einsatz gelangen. Dementsprechend ist SAP eine zentrale IT-Anwendung, in der umfangreiche Daten und Informationen verarbeitet und gespeichert werden. Grundlage für die Informationsverwaltung ist die Abbildung der Geschäftsarchitektur der jeweiligen Anwender. Dazu wird von der Abteilung Informationstechnik darauf hingewiesen, dass diese noch in Ausarbeitung ist.
Das Buchhaltungssystem wird von 1.037 Anwendern (inbegriffen der Südtiroler Landtag und die Regionalverwaltung), mit 354 zugewiesenen Rollen, verwendet. Das Personalverwaltungsprogramm wird von 255 Nutzern verwendet, denen 75 Rollen zugewiesen sind. Im Customer-Relationship-Management (CRM) sind vier unterschiedliche Rollen festgelegt.

Die Verwaltung der Nutzer und deren Monitoring nimmt einen wichtigen Stellenwert für das IKS ein (live cycle management). Laut Auskunft haben in den letzten 6 Monaten 212 Nutzer keinen Zugang zum Buchhaltungssystem durchgeführt, dies entspricht einem Prozentsatz von über 20 Prozent. Zum gegenwärtigen Zeitpunkt ist die jährliche Kontrolle der inaktiven Benutzer noch nicht durchgeführt worden.

Die Südtiroler Informatik AG (SIAG) trägt durch drei eigene Tätigkeitsfelder (Service Areas)[9] dieser Komplexität Rechnung. Es ist dies das Tätigkeitsfeld Human Resources Services, worin insbesondere das Human Capital Management (HCM) System und die Zeiterfassung der Landesverwaltung abgewickelt werden. Im Tätigkeitsfeld Finance & Accounting Services werden die Kernelemente Finanz- Bilanz- & Vermögensbuchhaltung, die Finanzverwaltung der Schulen, die Verwaltung des Schatzamtes, die Einsichtnahme des Steuereinzugsdienstes und die Verwaltung von Liquidierungen betreut. Im Tätigkeitsbereich Contribution & Payment Services werden die Ansuchen, als auch die Abwicklung von Beiträgen sowie die Zahlung von Steuern und Strafen unterstützt. Diese drei Tätigkeitsfelder werden durch ein SAP-Kompetenzzentrum (CoC) koordiniert. Das Kompetenzzentrum

[8] mit BLR vom 31.7.2000, Nr. 2852 ist die Ausschreibung “Neue Finanzverwaltung in der Landesverwaltung – SIC 07.2000” genehmigt worden, für welche sich eine Bietergemeinschaft bestehend aus IBM/SAP Consulting Italia den Zuschlag gesichert hat
[9] https://www.siag.it/de/service-areas

ist mit Fachexperten in SAP besetzt und auch mit spezifischen SAP-Projekten betraut. Die einzelnen Tätigkeitsfelder (Service areas) werden von einem Service Area Manager in der SIAG geleitet. Die Service Area Manager sind die unmittelbaren Ansprechpersonen der Demand Manager, welche direkt bei der Abteilung Informationstechnik angesiedelt sind und das Bindeglied zwischen der SIAG und den Fachabteilungen darstellen. Die zentrale Bedeutung der Demand Manager liegt in der Erhebung des Bedarfs an IT-Diensten (mit entsprechender Beratung) und in der Bestimmung des Bedarfs und der Anforderungen der Benutzer mit der Bewertung innovativer und kostensparender Lösungen[10].

Auf die Frage, wie das Zugangssystem zu den verschiedenen SAP-Anwendungen aufgebaut ist und auf welchen Betriebssystemen diese laufen, konnte erhoben werden, dass diese nicht einheitlich sind. So läuft die Finanzgebarung über AIX (IBM mit OS400) und die SAP-Haushaltsplanung über einen Windows Server 2016. Die Personalverwaltung, das CRM Modul und die Buchhaltung der Körperschaften und Schulen läuft über Windows NT.

Eine Arbeitsgruppe von Systemanalysten ist mit der Erstellung einer umfassenden Übersicht der SAP-Systemlandschaft betraut und befindet damit in der Fertigstellungsphase. Einzelne spezifische Anwendungen des SAP-Systems sind bereits in Diagrammen erfasst. Die Informationen über die SAP-Systemlandschaft sollen dem Kundensupport und allen Mitarbeitern dienen, um einen Überblick über die installierte Systemlandschaft und deren Kommunikationswege zu gewährleisten[11].

Die Funktionen eines SAP-Systems werden über Transaktionen aufgerufen, die unterschiedliche Operationen oder Aktivitäten (z.B. Schreiben, Lesen, Löschen) auf Daten ermöglichen. Die über Transaktionen gestarteten Anwendungen prüfen beim Aufruf, ob der aufrufende Benutzer über die notwendigen Berechtigungen verfügt, die angeforderte Operation auf den durch die Applikation angesprochenen Daten auszuführen[12]. Die Berechtigungen werden Benutzern dadurch gewährt, dass ihnen Rollen zugeordnet werden. Die Rollen geben an, welche Transaktionen durch den Benutzer ausgeführt werden können. Wichtig ist, dass Rollen letztendlich Arbeitsplätze oder Positionen beschreiben und nicht auf einzelne Mitarbeiter bezogen sind. Eine zu hohe Anzahl von Rollen kann andererseits wiederum zu Unübersichtlichkeit führen.
Die in SAP definierten Rollen der Landesverwaltung enthalten eine Grundbeschreibung der zugrunde liegenden Berechtigungen. So handelt es sich etwa bei der Rolle ZPABUFFENT um die Basisrolle für das Amt für Einnahmen. Die Rollen sind über zwei Kategorien definiert. Die Kategorie der Funktionsrollen ermächtigt, verschiedene Transaktionen durchzuführen und die Kategorie der Organisationsrollen ermöglicht es, für bestimmte Ämter/Abteilungen zu arbeiten.
Grundsätzlich geht es beim Berechtigungsmanagement also darum, ob und wie Benutzer oder IT-Komponenten auf Informationen oder Dienste zugreifen und diese benutzen dürfen. Aufgrund des zugewiesenen Benutzerprofils erhält dieser Zutritt, Zugang oder Zugriff. Das Berechtigungsmanagement bezeichnet die Prozesse, die für Zuweisung, Entzug und Kontrolle der Rechte erforderlich sind[13].
SAP hat das ABAP-Berechtigungskonzept[14] entworfen, welches Transaktionen, Programme und Services in SAP-Systemen vor unberechtigtem Zugriff schützen soll. Auf der Grundlage des Berechtigungskonzepts vergibt der Administrator den Benutzern Berechtigungen, die festlegen, welche Aktionen ein Benutzer im SAP-System ausführen darf, nachdem er sich am System angemeldet und authentifiziert hat.
Dem Benutzeradministrator kommt in diesem Kontext eine zentrale Rolle zu. Denn je nach Größe und Organisation übernimmt dabei ein einziger Administrator (Superuser) oder eine Gruppe von

[10] http://www.provinz.bz.it/de/kontakt.asp?orga_orgaid=7437
[11] https://de.wikipedia.org/wiki/System_Landscape_Directory
[12] https://www.processpartner.ch/wp-content/uploads/2017/03/1.1.5.3_2.-Leitfaden-SAP-Berechtigungen.pdf
[13] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html
[14] laut wikipedia ist **ABAP** eine proprietäre Programmiersprache der Softwarefirma SAP, die für die Programmierung kommerzieller Anwendungen im SAP-Umfeld entwickelt wurde und in ihrer Grundstruktur der Programmiersprache COBOL entfernt ähnelt

Administratoren die Berechtigungsvergabe und dessen Verwaltung.
Der Zugang zu den Anwendungen der Finanz- und Personalverwaltung durch die Benutzer erfolgt über SSO (Single Sign On), während für die restlichen Anwendungen dies noch nicht der Fall ist. Der SSO Zugang hat den Vorteil, dass mit einem einzigen Zugang sämtliche Anwendungen gestartet werden und damit nicht für jede Anwendung getrennt ein Passwort verwaltet werden muss. Damit verbunden sind auch eine geringere Anzahl von neuen Passwortanfragen an das Help Desk und damit geringere Kosten. Das SSO gewährt eine optimale Informationssicherheit, da zu jedem Zeitpunkt ermittelt werden kann, wer zu welchen Daten und zu welchen Zeitpunkt Zugang hatte. Weiters wird dadurch das Risiko reduziert, dass sich Dritte Zugang zum System verschaffen können. Die Gewährleistung der steten Betriebsbereitschaft und die Konfigurierung der verschiedenen Anwendungen für einen einzigen Zugang stellen erhebliche Herausforderungen an die Ressourcen (Personal, Finanzen) dar.

3.2. Ebene der Anwender

Bei der Berechtigung handelt es sich um eine Ermächtigung, bestimmte Aktionen im SAP-System durchzuführen[15]. Die Berechtigung ist daher von grundlegender Bedeutung für den ordnungsgemäßen Gebrauch der Anwendung. Ein Berechtigungskonzept schützt die Daten und Informationen vor Veränderungen oder Zerstörungen (Datensicherheit) und soll ihren unrechtmäßigen Gebrauch (Datenschutz) verhindern[16]. Die Produktivität des Systems darf unter diesen Rahmenbedingungen nicht eingeschränkt werden.

In der Landesverwaltung sind für die einzelnen Abteilungen universelle Rollen vorgesehen, die auf die jeweiligen Aufgaben der Stelleninhaber zugeschnitten sind. Spezifische Rollen sind für Schlüsselabteilungen (Abteilung Finanzen) eingerichtet worden, die ein breiteres Rollenspektrum abdecken bzw. transversale Funktionen ermöglichen. Damit wird dieser Abteilung ein erweiterter Zugang gewährleistet, der für die Abwicklung der Tätigkeit notwendig ist. Ansonsten beschränken sich die Rollen auf die jeweilige Fachabteilung.

Der Prozess des Benutzermanagements (life cycle management) wird teilweise über ein eigens von der Landesverwaltung erstelltes workflow gesteuert. Das von SAP zur Verfügung gestellte workflow kommt nicht zur Anwendung. Die Initiierung des Arbeitsablaufes erfolgt für Änderungen über die Öffnung eines Tickets oder über E-Mail des zuständigen Vorgesetzten bzw. der autorisierten Benutzer. Die Anforderungen um Änderungen werden für die Finanz- und Personalanwendungen direkt an das Kompetenzzentrum SAP (CoC SAP) übermittelt. Das Kompetenzzentrum seinerseits übermittelt, falls erforderlich, die Anfragen an die Systemadministratoren. Es wird eine Überprüfung der angeforderten Änderungen durchgeführt. Dieses Monitoring beinhaltet auch die Überprüfung der beantragten Änderungen hinsichtlich deren Ausmaßes und Auswirkungen. Diese dürfen normalerweise den jeweiligen Zugehörigkeitsbereich (Amt) nicht überschreiten, außer es handelt sich um spezifische Abteilungen. Jährlich wird ein audit über die verwendeten Lizenzen und die Benutzer durchgeführt.
Nach erfolgreicher Implementierung der angeforderten Rollen wird der Benutzer kontaktiert, um die erfolgreiche Ausführung nochmals zu eruieren.
Dieser Prozess wird mit dem SAP Solution Manager durchgeführt, eine von SAP entwickelte Anwendung, welche den Betrieb der installierten Applikationen unterstützt.
In den Richtlinien zur Verwendung der IT-Instrumente sind die Führungskräfte auf die Notwendigkeit der Mitteilung von Änderungen der Rollen oder Benutzer hingewiesen worden. Wenn abteilungsübergreifende Rollen beantragt werden, so wird eine entsprechende Autorisierung von den betroffenen Abteilungen angefordert.

Grundsätzlich sind die zugewiesenen Rollen auf die Mitarbeiter einer Abteilung zugeschnitten. Eine

[15] https://help.sap.com/saphelp_nwmobile71/helpdata/de/52/671285439b11d1896f0000e8322d00/content.htm?no_cache=true
[16] https://de.wikipedia.org/wiki/Berechtigungskonzept

Ausnahme bildet die Eingabe von Kunden und Lieferanten in das System, diese kann von allen autorisierten Benutzern durchgeführt werden. Eine nachfolgende Änderung dieser Daten ist jedoch nur durch das Amt für Einnahmen und das Amt für Ausgaben möglich.
Bei der Einführung von neuen Projekten (Transaktionen) werden die notwendigen Änderungen an den Rollen und den Benutzern gemeinsam mit der Fachabteilung abgeklärt und eingeführt. Es obliegt jedenfalls der Fachabteilung dies zu bestimmen. Rollen selbst können nur vom Kompetenzzentrum SAP, von den Systemadministratoren und den technischen Assistenten der Systemadministratoren neu eingefügt werden.

Was die Anwendung der allgemeinen Sicherheitsrichtlinien und des Passwortschutzes anbelangt, so werden die Passwortänderungen im System durchgeführt. Genauso erfolgt eine Blockierung des Benutzers nach einer bestimmten Anzahl von erfolglosen Login Versuchen. Die Anzahl dieser erfolglosen Versuche ist derzeit mit fünf festgelegt. Die Benutzer können das Passwort jederzeit zurücksetzen, jedoch nicht öfter als ein Mal pro Tag. Das neue Passwort muss verschieden von den fünf vorher benutzten Passwörtern sein. Die Systemadministratoren können, auf spezifische Anweisung des Vorgesetzten, den Nutzer oder Funktionalitäten sperren. Der normale Gültigkeitszeitraum eines Passwortes beläuft sich auf 90 Tage. Dort wo der SSO Zugang realisiert ist, gelten die Regeln der active directory, andernfalls muss eine entsprechende Anfrage gestellt werden. Die active directory ermöglicht es, ein Netzwerk entsprechend der realen Struktur des Unternehmens oder seiner räumlichen Verteilung zu gliedern[17]. Damit können verschiedene Objekte (Benutzer, Server, Drucker) verwaltet werden. Weiters kann ein Administrator die Informationen der Objekte organisieren, bereitstellen und überwachen.

Ein weiterer sicherheitsrelevanter Aspekt betrifft die kontinuierliche Ajourierung der von SAP und (Microsoft) gelieferten Sicherheits-Patches. Diese sollen mögliche aufgetretene Fehler beheben - insbesondere auch Sicherheitslücken - schließen. Diese Korrekturlieferungen werden, im Rahmen der Produktverfügbarkeit von SAP im Betrieb, übernommen.

Die Trennung in verschiedene Funktionsgruppen von Anwendern erfolgt über die Zuweisung der Lizenzen an die jeweiligen Strukturen. Für diese können auch eigene Gruppen gebildet werden. Derzeit sind die entsprechenden Rollen aufgrund der Bedürfnisse der Benutzer gebildet und werden transversal zugewiesen.

Was hingegen die Erfassung von kritischen Funktionen anbelangt und ein dazugehöriges Regelwerk für Funktionstrennungen, so ist derzeit eine Revision der Rollen in Durchführung, welche insbesondere im Bereich der Administratoren eine Trennung von Systemadministratoren, Entwicklern und externen Entwicklern vorsieht. Dieselben Anpassungen sind für Sonder-/Notfallbenutzer in der Durchführungsphase.

3.3. Ebene der Administratoren

Administratoren haben die Aufgabe, Computersysteme und Netzwerke zu betreuen. Aufgrund ihrer umfangreichen Rechte in der Verwaltung von Computersystemen und Netzwerken kommt ihnen eine besondere Bedeutung zu. Eine besondere Kategorie von Administratoren hat SAP mit Super-User eingerichtet, die unabhängig von ihrer Funktion, auf das gesamte System Zugriff haben und darauf arbeiten können. Für ein funktionierendes IKS ist die Ausgestaltung der organisatorischen Regeln in diesem Bereich ausschlaggebend.

Derzeit haben die Systemadministratoren des Bereiches RUN in der SIAG die umfangreichen Rechte eines Superusers zugewiesen bekommen und können daher direkt auf das System zugreifen. Die

[17] https://de.wikipedia.org/wiki/Active_Directory

Mitarbeiter des Kompetenzzentrums SAP können Rollen erstellen und an die Nutzer zuweisen. Derzeit wird eine Überprüfung dieser Zuteilung durchgeführt, mit dem Ziel eine punktuellere Zuweisung der Aufgaben in diesem Bereich zu erreichen. Vorgesehen ist dabei auch die Einführung einer spezifischen Rolle für die Verwaltung der Benutzer und der Autorisierung der Rollen.

Transaktionen können ausschließlich von Entwicklern und Systemadministratoren angelegt und abgeändert werden. Kein anderer Benutzer hat die Berechtigung Transaktionen zu entwickeln und einzufügen, auch wenn er den entsprechenden Kodex kennen würde. Gleichfalls können nur die Systemadministratoren und Entwickler Autorisierungen für die Nutzung vergeben.

Was den Zugriff auf als kritisch eingestufte Transaktionen und Tabellen anbelangt, so hängt dies von den entsprechenden Transaktionen ab. Diese werden nur von den Systemadministratoren verwaltet. Insgesamt sind in SAP eine beträchtliche Anzahl von Transaktionen vorgesehen. Die Systemadministratoren und Entwickler haben Zugang zu allen Transaktionen. Im neuen System CRM und S/4 werden drei Typen von Rollen vorgesehen:

- Systemadministrator, ohne Einschränkungen da Verwalter des Systems
- Entwickler, mit der Entwicklung von Transaktionen, auch funktionale Transaktionen für die Kollaudierung beauftragt
- Funktionsadministratoren für die ausschließlich vorgesehenen Transaktionen im Rahmen der zugewiesenen Rolle und mit den spezifischen organisatorischen Einschränkungen.

In Bezug auf das Berechtigungs- und Zugriffsmanagement ist die Abteilung darauf orientiert, eine strukturiertere Abwicklung der Anfragen über Key2help zu implementieren. Zusätzlich sollen in den neuen Systemen CRM und S/4 Rollen für jede Kategorie von Nutzern vorgesehen werden.

IV. Bewertungen und Empfehlungen

Die SAP-Anwendungen sind in der Südtiroler Landesverwaltung und deren abhängigen Körperschaften fundamentale Bestandteile des Informationssystems. In diesen Systemen sind zahlreiche Informationen gespeichert, die es nach den geltenden gesetzlichen Bestimmungen (Datenschutz) zu verwalten und zu schützen gilt (Datensicherheit). Dieser Schutz ist sowohl nach außen als auch nach innen zu gewährleisten. Ein auf die betrieblichen Erfordernisse abgestimmtes Berechtigungs- und Zugriffsmanagement unterstützt dabei die Verwaltung in der Ausübung dieser Vorgaben und Richtlinien.
Derzeit laufen die SAP-Anwendungen auf verschiedenen Betriebssystemen, was verständlicherweise eine große Herausforderung für die Gewährleistung der Informationssicherheit darstellt. Die Vereinheitlichung der Systeme stellt auch eine große finanzielle Herausforderung dar und unterliegt der strategischen Entscheidung des Betriebes.
Die SAP-Anwendungen bieten selbstverständlich bereits in der technischen Grundausstattung verschiedene Lösungsmöglichkeiten an. Diese Voreinstellungen können vom Betrieb individuell ausgestaltet werden unter Berücksichtigung der grundsätzlichen Elemente des internen Kontrollsystems im Berechtigungs- und Zugriffsmanagement. Dabei wird die Anwender- als auch die Administratorenebene unterschiedlich reglementiert. Besonderes Augenmerk wird den sogenannten Superusern gewidmet, die einen uneingeschränkten Zugang zum System haben können.

Aus den übermittelten Unterlagen und den daraus gewonnenen Informationen kann das grundsätzliche Bewusstsein über die Bedeutung des Berechtigungs- und Zugriffsmanagements, auch hinsichtlich der wirkungsvollen Ausgestaltung eines IKS, festgestellt werden.
Es wird begrüßt, dass die Abbildung der SAP-Systemlandschaft sich in der Fertigstellungsphase befindet und damit die Implementierung des IKS in jedem Bereich erleichtert wird. Dazu gehört auch die Verschriftlichung der zugrunde liegenden Geschäftsprozesse, auch unter Miteinbeziehung der demand manager.

Vorwiegend wird bereits der Zugang zu den Systemen über SSO gewährleistet und bietet damit eine sehr gute Kontrolle des Berechtigungs- und Zugriffsmanagements. Ausgereift ist der Zugang zu den Systemen durch die gut ausgestaltete Passwortverwaltung.
Zu verstärken, auch in zeitlicher Hinsicht, sind die Überprüfungen inaktiver Benutzer und die darauffolgenden Abmeldungen vom System. Diesbezüglich würde es sich anbieten, die Fachabteilungen in diese Überprüfungen verstärkt mit einzubeziehen. Ein einziges informationsgestütztes Management der Benutzerverwaltung unter Berücksichtigung der Trennung von Antrag, Freigabe, Durchführung und Bestätigung (workflow) wäre empfehlenswert für ein effektives *life cycle* management.

Für ein gut funktionierendes IKS im Berechtigungs- und Zugriffsmanagement ist es unerlässlich, ein Gleichgewicht zwischen einer differenzierten Ausgestaltung der erforderlichen Rollen und einer Überzahl von Rollen zu finden. Auf der Anwenderseite sind derzeit eine große Anzahl von Rollen (354) festgelegt. Es wird empfohlen, eine eingehende Analyse der Anzahl und Inhalte der Rollen durchzuführen.
Begrüßt wird die Überarbeitung der bestehenden Rollenprofile auf Ebene der Administratoren, auch die Anpassung im Bereich der Sonder-/Notfallbenutzer. Dieser Bereich verdient aufgrund seiner Bedeutung besondere Aufmerksamkeit.
Die schriftliche Festlegung dieser Aufgaben verstärkt den Reifegrad eines funktionierenden IKS. Empfehlenswert wäre auch die einheitliche Festlegung für die Erstellung der Datenbank im Bereich Kunden und Lieferanten, damit mehrmalige Stammdatensätze vermieden werden.

Ein Follow up im Jahr 2021 wird die Umsetzung der Empfehlungen erheben.

Abschließend wird ein Dank an die Abteilung Informationstechnik für die gute Zusammenarbeit - auch aufgrund der besonderen Herausforderung durch die Corona Pandemie - gerichtet.

Eva Maria Kofler

Firmato digitalmente da:Eva Maria Kofler
Data:18/09/2020 10:41:40

Martin Steinmann

Digitally signed by: Martin Steinmann
Date: 18/09/2020 10:32:32

Prüfstelle
39100 Bozen | Freiheitsstraße 66
Organismo di valutazione
39100 Bolzano | Corso Libertà, 66

Tel. 0471 402 212 | Fax 0471 260 114
pruefstelle@landtag-bz.org | organismodivalutazione@consiglio-bz.org
PEC: pruefstelle.organismovalutazione@pec.prov-bz.org
www.landtag-bz.org/de/pruefstelle.asp
www.consiglio-bz.org/it/organismo-di-valutazione.asp