

Admin-Richtlinie V2.1.doc
13.06.2005

Regelung für die Administratoren der informationstechnischen Systeme des ZDF

Schwerpunkte: Administratoren-Account und
Verantwortlichkeiten für IT-Sicherheit und Datenschutz

Juni 2005

Inhaltsverzeichnis

1	Grundlagen	3
1.1	Zweck der Regelung	3
1.2	Rahmenbedingungen	3
2	Teil A – übergreifende Regelungen	4
2.1	Organisation des Administratorenwesens	4
2.1.1	Verantwortlichkeiten für IT-Sicherheit und Datenschutz	4
2.1.2	Protokollierung, Erfassungsvorgaben	5
2.1.3	Schutz des Administrators und Verfahrensweg bei Verdacht- und Missbrauchfällen	5
2.2	Administratoren-Account	6
2.2.1	Erfassungsstruktur für Rechte und Merkmale von Administratoren	6
2.2.2	Erlangung eines Administratoren-Account	7
2.2.3	Löschung und Änderung eines Administratoren-Account	8
2.3	Tätigkeiten von Administratoren	8
2.3.1	Hoch- und Herunterfahren von Systemen	9
2.3.2	Installation, Konfiguration und Freischalten	9
2.3.3	Datensicherung und Rücksicherung	10
2.3.4	Betriebsüberwachung	10
2.3.5	Benutzerbetreuung und Störungsbeseitigung	10
2.3.6	Benutzerverwaltung	10
2.3.7	Verwaltung von Arbeitsplatzrechnern	11
3	Teil B – spezifische Regelungen	11
3.1	Berücksichtigte Besonderheiten des ZDF	11
3.2	Spezifische Regelungen und Einschränkungen	12
3.2.1	Allgemeine Regelung	12
3.2.2	Systemadministratoren	12
3.2.3	Applikationsadministratoren (systemverantwortliches IT-Personal)	13
3.2.4	Applikationsadministratoren (in den Fachbereichen)	13
3.2.5	Administratoren für sendenahe Systeme	14
3.2.6	Administratoren für Arbeitsplatzrechner (IT-Personal)	14
3.2.7	Lokale Administratoren (Benutzer)	14
4	Verpflichtungserklärung	15
5	In-Kraft-Treten	15

1 Grundlagen

1.1 Zweck der Regelung

Zweck dieser Regelung für Administratoren ist die Erfüllung der einschlägigen Richtlinien zur IT-Sicherheit und zum Datenschutz unter Berücksichtigung der Ziele und Aufgaben des ZDF. Hier geregelt werden die Struktur und generelle Merkmale des Administratorenwesens des ZDF sowie die Pflicht zur Dokumentation von Administratorenberechtigungen und transparenten Verfahrensweisen. Nicht geregelt werden die Pflichten von Administratoren im Einzelnen.

1.2 Rahmenbedingungen

Es gelten die Bestimmungen des Landesdatenschutzgesetzes Rheinland-Pfalz (LD SG). Über die gesetzlichen Bestimmungen hinaus finden sich im IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnologie einschlägige Empfehlungen. Diese werden hiermit als maßgeblicher Leitfaden für das ZDF festgeschrieben.

Ebenso gelten die vom IT-Sicherheitsbeauftragten herausgegebenen "Sicherheitshinweise für Administratoren im ZDF" in der jeweils aktuell gültigen Fassung. Zur Verbesserung der Transparenz und im Einklang mit den somit für das ZDF geltenden Bestimmungen und Leitfäden werden an dieser Stelle die folgenden generellen Ziele hervorgehoben:

- generelles Ziel ist die Transparenz des Administratorenwesens,
- strukturierte Zuweisung der Verantwortlichkeit für IT-Sicherheit und Datenschutz,
- korrekte und aktuelle Listen sowie Recherchemöglichkeiten zu einschlägigen Berechtigungsinformationen,
- Begrenzung von Berechtigungen auf das zur Aufgabenerfüllung Notwendige (Umfang und Dauer),
- Multiuser sind nicht erlaubt, Ausnahmefälle werden dokumentiert und begründet (mehr als einer Person zur Ausübung von Administratorentätigkeiten zugewiesener Zugang zu einem IT-System),
- Vermeidung von gebündelten Berechtigungseinträgen für separate Anwendungsbereiche, die einem einzigen Administratoren-Zugang zugewiesen werden.

2 Teil A – übergreifende Regelungen

2.1 Organisation des Administratorenwesens

2.1.1 Verantwortlichkeiten für IT-Sicherheit und Datenschutz

Zentrale Anlaufstelle für IT-Sicherheit und Datenschutz sind zum einen der **IT-Sicherheitsbeauftragte** und zum anderen der **Datenschutzbeauftragte** des ZDF. Die in diesen Funktionen beauftragten Personen beraten Geschäftsführung und IT-betreuende Bereiche des ZDF bei der Organisation der IT-Infrastruktur. Dabei bereiten sie ZDF-bezogene Grundlagen und Richtlinien vor, die dann von der Geschäftsführung und in Abstimmung mit dem Personalrat in Kraft gesetzt werden.

IT-Sicherheitsbeauftragter und Datenschutzbeauftragter werden in ihren Funktionen durch die IT-betreuenden Bereiche unterstützt. Hierzu zählt die Einsetzung eines verantwortlichen **IT-Sicherheitsmanagers** zu einem IT-betreuenden Bereich oder die Wahrnehmung dieser Funktion durch den jeweiligen Geschäftsfeldleiter selbst. Der IT-Sicherheitsmanager verantwortet auf operationeller Ebene die auf sein Geschäftsfeld bezogene Dokumentation von Administratorenberechtigungen und transparenter Verfahrensweisen im Einklang mit dieser Regelung.

Zur Umsetzung der Regelung für Administratoren durch den IT-Sicherheitsmanager zählt insbesondere:

- Anlage und Pflege einer Administratorenliste auf Basis der Strukturierungselemente gemäß Ziffer 2.2.1, die den Ist-Zustand der Administratorenberechtigungen im jeweiligen Geschäftsfeld dokumentiert,
- Funktion des gemäß Ziffer 2.2.2 mindestens einzubeziehenden Genehmigungsberechtigten,
- Beschreibung von Ausnahmefällen, in denen Administratorenrechte außerordentlich vergeben werden, und Mitwirkung an möglichen Notfallplänen,
- Überprüfung und ggf. Initiierung der Löschung oder Änderung von Administratoren-Accounts gemäß Ziffer 2.2.3,
- Vorgabe bereichsspezifischer Verfahrensweisen und Handlungsanweisungen unter Einbeziehung aller betroffenen Beschäftigten in folgenden Punkten:
 - Formale Vorgehensweise bei der Erlangung eines Administratoren-Account,
 - Festlegung der anzuwendenden Prinzipien zu den in Ziffer 2.2.3 aufgelisteten Abwägungskriterien,
- Überwachung datenschutz- und sicherheitsrelevanter Erfassungsvorgänge in Bezug auf die operationelle Administratorentätigkeit gemäß Ziffer 2.1.2.

Generell ist jedes Geschäftsfeld bezüglich der in seinem Bereich betreuten Informationstechnologie sowohl für die fachliche Konkretisierung der hier getroffenen Regelungen wie auch für deren organisatorische Umsetzung und Überwachung verantwortlich.

2.1.2 Protokollierung, Erfassungsvorgaben

Die Protokollierung von Administratorentätigkeiten und der Umfang der dabei in sogenannten Log-Dateien erfassten Daten dient ausschließlich dem Zweck der IT-Sicherheit und dem Datenschutz.

Lassen sich etwa Schadensfälle, Missbrauchsfälle von personenbezogenen Daten oder die begründete Erwartung, dass diese eintreten, auf bestimmte IT-Systeme eingrenzen, so soll es Protokollierungen geben, aus denen hervorgeht, welche Administratoren-Accounts zuletzt genutzt wurden. Ein hoher Schutz dieser Protokollierungen selbst soll unter Beachtung der technischen Möglichkeiten (z. B. zentrale, verschlüsselte Speicherung von Log-Dateien) und der damit verbundenen Kosten erzielt werden. In Log-Dateien werden im Regelfall zumindest die nachfolgenden Daten pro erfolgtem Anmeldevorgang erfasst.

- Account-Anmeldename
- An- und Abmeldezeitpunkt
- Ausgangspunkt des Anmeldevorgangs - lokal oder über Netzwerk (remote)
- Bei Netzwerk-Einwahl: Name der Ausgangsmaschine (wo der Administrator ist)

Dem Datenschutzbeauftragten, Personalrat und/oder dem IT-Sicherheitsbeauftragten ist auf deren Verlangen und unter Einbeziehung des verantwortlichen IT-Sicherheitsmanagers der Zugang zu allen verfügbaren Log-Dateien zu gewähren.

2.1.3 Schutz des Administrators und Verfahrensweg bei Verdacht- und Missbrauchsfällen

Der Umfang der erfassten Daten wird im Regelfall auf die in Ziffer 2.1.2 benannten Daten beschränkt. Ausnahmefälle sind zu dokumentieren und zu begründen. Dabei müssen die Interessen der IT-Sicherheit gegenüber den berechtigten Interessen der betroffenen Personen abgewogen werden. Administratoren müssen über die Details der sie im Einzelfall betreffenden Protokollierungsmechanismen in Kenntnis gesetzt sein.

Die personenbezogene Auswertung von Log-Dateien ist ausschließlich aus begründetem Anlass und gebunden an den Zweck der IT-Sicherheit und des Datenschutzes erlaubt. Ist ein solcher Anlass gegeben, so muss bei der Auswertung der Log-Dateien mindestens der verantwortliche IT-Sicherheitsmanager sowie ein weiterer Bearbeiter nach dem Vier-Augen-Prinzip miteinbezogen werden. Eine Leistungs- und Verhaltenskontrolle auf Basis der Protokolldaten ist nicht zulässig.

Nachträgliche Manipulationen an Log-Dateien sind strikt untersagt. Alle Personen, die Zugang zu Log-Dateien mit personenbezogenen Daten Dritter haben, unterliegen der unter Ziffer 4.1 in Bezug genommenen Verpflichtungserklärung. Der unkontrollierte Zugang zu Log-Dateien ist zudem mit technischen Mitteln, soweit möglich und wirtschaftlich vertretbar, zu verhindern.

Trotz technischer Vorkehrungen und Dienstanweisungen können technische Fehler, menschliches Versagen oder auch gezielte Manipulationen zu Situationen führen, in denen auf Schadensfälle, Missbrauchsfälle von personenbezogenen Daten oder die begründete Erwartung, dass diese eintreten, unerwartet reagiert werden muss. Da die Abwehr weiterer Schäden oder Gefahren zumeist ein schnelles Handeln erfordert, müssen alle IT-betreuenden Bereiche die entsprechenden Vorgaben der "Sicherheits-

hinweise für Administratoren im ZDF“, die der IT-Sicherheitsbeauftragte in geeigneter Weise zugänglich macht, erfüllen (siehe Ziffer 1.2).

Bei Verdacht auf missbräuchliche/unerlaubte Nutzung von Administratorenrechten erfolgt unter Beteiligung des Datenschutzbeauftragten eine Überprüfung durch den IT-Sicherheitsbeauftragten. Über festgestellten Missbrauch oder gravierende Missbrauchsversuche ist der zuständige Personalrat zu informieren.

2.2 Administratoren-Account

Der konkrete Zugang von Administratoren zu den ihnen zugewiesenen Berechtigungen wird über sogenannte Administratoren-Accounts in den jeweiligen IT-Systemen und Applikationen realisiert. Eine systematische Dokumentierung dieser Administratoren-Accounts ist damit der wichtigste Beitrag zur Transparenz des Administratorenwesens. Ziel ist eine gesicherte Ermittlung

- a) aller Personen und Rechte, die sie ausüben, **zu einem IT-System** sowie
- b) aller zugeordneten IT-Systeme und der dort zugewiesenen Rechte **zu einer Person**.

Eine Nachverfolgung und Ermittlung dieser Zuordnungsverhältnisse im Einzelfall wird durch den Datenschutzbeauftragten des ZDF initiiert, wenn er nach Maßgabe des Datenschutzes einen Vorfall verfolgt, Stichproben empfiehlt oder Informationen sammelt, die der Überprüfung der generellen Rahmenbedingungen (Ziffer 1.2) dienen. Eine Nachverfolgung und Ermittlung dieser Zuordnungsverhältnisse dient ebenfalls dem IT-Sicherheitsbeauftragten des ZDF bei Sicherheitsvorfällen und generell den systembetreuenden Bereichen zur Handhabung und Weiterentwicklung des Administratorenwesens.

2.2.1 Erfassungsstruktur für Rechte und Merkmale von Administratoren

Die IT-Systeme des ZDF auf der einen und die Personen auf der anderen Seite werden über Administratoren-Accounts zueinander in Beziehung gesetzt. Die folgenden Begriffe und Elemente werden bei der Erfassung dieser Beziehungen verwendet.

Da die IT-Systeme im ZDF sehr unterschiedlich sind, werden sie **Systemkategorien** (z. B. Windows-/Unix-Server, Host, Arbeitsplatzrechner etc.) und daneben **ggf. Systemgruppen** zugeordnet.

Mit Systemgruppen lässt sich die Zugehörigkeit zu übergeordneten IT-Systemen oder Applikationen bzw. Services darstellen. Jedem einzelnen **IT-System** ist für seine eindeutige Erfassung eine eigene Bezeichnung zugeordnet.

Ein Administratoren-Account ist ein mit einem IT-System verbundener und in diesem festgelegter Berechtigungseintrag. Ein solcher Administratoren-Account besteht aus einem Anmeldenamen und einem Passwort. Die Authentifizierung bei der Benutzung des Accounts findet dabei entweder durch das IT-System selbst oder über ein zentrales Berechtigungssystem statt.

Mehrere Administratoren-Accounts können im IT-System darüber hinaus einer **Berechtigungsgruppe** zugeordnet sein, über die jedem dieser Accounts gemeinsame Berech-

tigungen zugeordnet werden. Zur inhaltlichen Erfassung eines Account oder einer Berechtigungsgruppe zählt eine Aufzählung und Beschreibung der zugeordneten Berechtigungen.

Die eindeutigen Bezeichnungen für IT-Systeme und Accounts werden dokumentiert und ermöglichen so eine systematische Recherche des IT-Systems zu einem vorgegeben Account und umgekehrt aller Accounts und mit diesen festgelegten Berechtigungen zu einem IT-System.

Der Bezug zu den realen Personen, den Administratoren, wird über eine Verbindung zwischen jeweiligem Account und Person dokumentiert. Dabei dürfen einer Person mehrere Accounts, umgekehrt einem Account aber nur in begründeten Ausnahmefällen mehrere Personen zugeordnet sein (Multiuser-Account). Mit dieser Erfassungsstruktur werden Personen mit IT-Systemen und den darauf ausgeübten Berechtigungen in Beziehung gesetzt.

Zu den personenbezogenen Erfassungsdaten zählen neben dem Personennamen eine Kennzeichnung ob **interner oder externer Mitarbeiter** sowie darüber hinaus für jeden zugeordneten Account eine **Begründung** und eine zeitliche **Befristung**. Aus der Begründung soll insbesondere die dienstliche Notwendigkeit hervorgehen.

2.2.2 Erlangung eines Administratoren-Account

Die Vergabe eines Administratoren-Account muss über eindeutig definierte Genehmigungsverfahren ablaufen. Die im jeweiligen Umfeld sachgerechte Ausgestaltung liegt in der Verantwortung der systembetreuenden Bereiche, wobei die folgenden übergreifenden Bedingungen zu erfüllen sind:

- Administratoren-Berechtigungen sind schriftlich zu beantragen.
- Die Beantragung ist mit der dienstlichen Notwendigkeit und Angaben zum Aufgabenbereich zu begründen und durch mindestens einen verantwortlichen ZDF-Beschäftigten (Genehmigungsberechtigter) zu genehmigen.
- Die in den Vorgang einbezogenen Genehmigungsberechtigten vergewissern sich, dass
 - die beantragte Berechtigung für die Erfüllung der Aufgaben des Administrators benötigt wird und ggf. früher erteilte Berechtigungen nicht genügen,
 - alternativ kein reduzierter Berechtigungsumfang praktikabel ist und
 - der Administrator mit seinem Wissensstand geeignet ist.
- Der Administrator wird formal verpflichtet,
 - die ihm persönlich übertragenen Berechtigungen nur für die Erfüllung seiner dienstlichen Aufgaben zu nutzen und diese nicht Dritten zu übertragen,
 - Passwörter geheim zu halten und umsichtig zu verwahren,
 - eine Auswertung von Protokollen mit personenbezogenen Daten grundsätzlich zu unterlassen, ein in Ausnahmefällen nötiger Zugriff auf Protokolle mit personenbezogenen Daten darf nur unter Beachtung der einschlägigen Datenschutzrichtlinien und dem LpersVG Rheinland-Pfalz erfolgen,
 - selbst Administratoren-Rechte nur nach Maßgabe der Regelungen in diesem Dokument zu vergeben,

- nicht-administrative Aufgaben nicht unter Verwendung des Administratoren-Account auszuführen.

Abweichend von dem hier behandelten Genehmigungsverfahren darf ein Administratoren-Account nur in begründeten Ausnahmefällen, etwa in Notfällen oder zur Abwendung offensichtlich sonst unvermeidbarer Schadenssituationen, vergeben werden. Derart übertragene Berechtigungen müssen eng befristet und dokumentiert werden. Verantwortlichkeiten und Vorgehenspläne werden von den jeweils systembetreuenden Bereichen bestimmt.

2.2.3 Löschung und Änderung eines Administratoren-Account

Die Administratorenberechtigungen unterliegen einer zeitlichen Befristung, die bei ihrer Vergabe jeweils festzulegen ist. Es ist Aufgabe der systembetreuenden Bereiche, sie regelmäßig auf ihre weitere Notwendigkeit hin zu überprüfen. Alle Stellen des ZDF sind zu den notwendigen Auskünften verpflichtet. Die systembetreuenden Bereiche sind dafür verantwortlich, dass die Anforderungen von IT-Sicherheit und Datenschutz mit vertretbarem Aufwand berücksichtigt werden.

Entsprechend begründet und sachverständig abzuwägen sind

- die generellen Befristungsregeln für Administratoren-Accounts
- der Turnus zur Überprüfung der in den Systemen angelegten Accounts (im Regelfall soll diese Art der Überprüfung einmal pro Jahr erfolgen, Ausnahmeregeln sind zu begründen und zu dokumentieren)
- Einzelmaßnahmen und Sicherheitstests (bei großen Datenmengen sind korrekte und aktuelle Listen nur über automatisierte Verfahren gewährleistet; das gilt insbesondere für die Überprüfung der Berechtigungen der lokalen Administratoren)
- der Vollzug der Rücknahme nicht oder als abgelaufen dokumentierter Administratoren-Berechtigungen in den IT-Systemen.

Ändern sich die Voraussetzungen für den Bestand oder den Umfang einer Berechtigung, insbesondere in Folge von innerbetrieblichem Arbeitsplatzwechsel, Veränderungen der Aufgaben oder Ausscheidens aus den Diensten des ZDF, werden die entsprechenden Administratoren-Accounts angepasst. In diesen Fällen haben die veranlassenden Bereiche den systembetreuenden Bereichen die für die Anpassung der Accounts notwendigen Angaben zu liefern. Die HA-Personal meldet das Ausscheiden von Mitarbeitern.

2.3 Tätigkeiten von Administratoren

Die Administratoren der IT-Systeme des ZDF werden nach folgenden Typen geordnet:

- **Systemadministratoren**
Aufgabenbereich ist der Betrieb der zentralen IT-Infrastruktur des ZDF, bestehend aus Großrechner, Server-Rechnern, Speichersystemen, Netzwerktechnik und Netzzugangsrechnern sowie sogenannten Domänen.

- **Applikationsadministratoren** (Rechte innerhalb von Softwarelösungen)
 - Systemverantwortliche Applikationsadministratoren (i. d. R. Applikationsentwickler, die nach Inbetriebnahme von Applikationen auch Wartungs- und Weiterentwicklungsaufgaben übernehmen)
 - Applikationsadministratoren in den Fachbereichen, die mit den Systemen arbeiten (i. d. R. zuständig für die Vergabe von Zugangs- und Nutzungsrechten im Fachbereich)

Unter Applikationen werden hier ZDF-spezifische Softwarelösungen verstanden, die auf fachbezogene Aufgaben ausgerichtet sind und einem Nutzerkreis zur Verfügung gestellt werden. Die Rechte von Applikationsadministratoren sind auf Applikationen, das heißt, die auf Großrechner oder Server-Rechnern ablaufende Software bezogen.
- **Administratoren für sendenahe Systeme**

Administrierte IT-Systeme sind z. B. DPA, DBC, digitale Archive, Schnittsysteme, Sendeablaufsteuerung oder Teletextrechner.
- **Administratoren für Arbeitsplatzrechner**

Das sind die mit IT-Aufgaben betrauten Beschäftigten.
- **Lokale Administratoren**

Das sind Benutzer mit Administratorenrechten auf selbst genutzten Arbeitsplatzrechnern.

Administratoren müssen für die Ausübung ihrer Tätigkeiten über weitgehende Berechtigungen verfügen. Um einem Verbleib von Rechten, die aufgrund personeller und organisatorischer Veränderungen reduziert werden könnten, entgegen zu wirken und zur Begrenzung von Berechtigungen auf das Notwendige wird im Abschnitt 2.2.3 mit den Regelungen zu Löschung und Änderung eines Administratoren-Account die systematische Überprüfung aller Berechtigungen beschrieben.

Zur Eingrenzung des Gegenstands derartiger Überprüfungen müssen sich alle Administratorentätigkeiten grundsätzlich aus den wie folgt generalisierten Basistätigkeiten ableiten.

2.3.1 Hoch- und Herunterfahren von Systemen

Gezieltes und geordnetes Hochfahren des Systems bzw. Herunterfahren des Systems mit Berücksichtigung aller Subsysteme und Schnittstellen zu Vor- und Nach-Systemen. Zu beiden Aufgaben gehört das Benachrichtigen der Servicemanager der Vor- und Nach-Systeme über jeden geplanten und erfolgten Start und Stopp des Systems.

2.3.2 Installation, Konfiguration und Freischalten

Installation: Einrichten des Systems. Installieren von Hardware, Software, Patches, Upgrades etc. für das System.

Re-Konfiguration: Verändern der Konfiguration bzw. Parameter-Einstellungen (z. B. Dateigrößen) eines bereits produktiven Systems oder dessen Umgebung. Installation und Re-Konfiguration verändern das produktive System oder seine Umgebung auf der Basis definierter Vorgaben.

Freischalten: Mitwirken beim Abnahme-Test einer Installation oder Re-Konfiguration. Technisches Freischalten der neuen System-Konfiguration, sobald die Freigabe für

den produktiven Betrieb erteilt wurde. Dokumentieren und kommunizieren der freigegebenen Version.

2.3.3 Datensicherung und Rücksicherung

Sichern und Rücksichern von Daten auf Band oder andere Langfrist-Datenträger für das System.

2.3.4 Betriebsüberwachung

Sicherstellen der Verfügbarkeit des Systems. Die zu überwachenden Eigenschaften und die zulässigen Werte oder Schwell- und Alarmwerte sowie die dadurch angestoßenen Aktionen werden in einem Betriebskonzept definiert. Bei den Aktionen kann es sich um reaktive, wenn ein Fehler eingetreten ist, oder pro-aktive, wenn sich ein potenzielles Problem abzeichnet, Maßnahmen handeln.

2.3.5 Benutzerbetreuung und Störungsbeseitigung

Die Benutzerbetreuung leistet einen Beitrag zur Erkennung von Störungen oder Handlungserfordernissen. Wesentliche Tätigkeiten der Administratoren ergeben sich durch deren Mitwirkung bei der Störungsbearbeitung und Wiederherstellung des reibungslosen Betriebs.

Die Benutzerbetreuung gliedert sich in drei Stufen,

die erste Stufe (bezeichnet als 1st Level Support bzw. Helpdesk) kommt zunächst ohne technische Unterstützung aus und dient der Kontaktaufnahme und Beantwortung häufig gestellter Fragen.

Die zweite Stufe (2nd Level) wird bei Bedarf hinzugezogen und dient der Beantwortung spezieller Fragen und falls nötig einer tiefergehenden Fehler-Lokalisation und Behebung.

Die Aufgabe des 3rd Level Support (Unterstützung des 2nd Level Support) übernehmen in der Regel Applikationsadministratoren, ggf. auch externe Dienstleister.

2.3.6 Benutzerverwaltung

Basisaufgaben sind Benutzer anlegen/löschen/freischalten/sperrern sowie Benutzer-Stammdaten, Zugriffsrechte und Passwörter pflegen.

Die Vergabe von Zugriffsrechten kann selbst Rechte zur Ausübung von Administrator-tätigkeiten behandeln und setzt dann ihrerseits weitgehende Administratorenrechte voraus („Super-Administrator“).

Abgesehen von der Pflege der Administratorenrechte beschränkt sich die Zuständigkeit der Systemadministratoren i. d. R. auf netzbezogene Rechte. Sie vergeben Zugriffsrechte für Netz-Zugang, E-Mail-Postfach, Home- und Gruppenlaufwerke oder legen Benutzerzugänge an (User-ID), deren spezifische Rechte dann von anderer Stelle eingerichtet werden.

Die Applikationsadministratoren vergeben i. d. R. Rechte zum Zugriff auf Applikationen, die teils beschränkt auf das Lesen und Recherchieren von Informationen sein können, oder die zum Betrieb und zur Pflege von Applikationen und Datenbankinhalten benötigt werden.

Den Zugang zu Applikationen verwalten häufig die Fachbereiche selbst.

2.3.7 Verwaltung von Arbeitsplatzrechnern

Arbeitsplatzrechner sind alle PC, Laptops und sonstige PC-ähnlichen Datenverarbeitungseinrichtungen des ZDF am Arbeitsplatz wie auch im Produktionseinsatz. Administratoren für Arbeitsplatzrechner erweitern und verändern Softwareinstallationen dieser Geräte.

Neben professionellen IT-Beschäftigten, die diese Tätigkeiten zur Betreuung der IT-Nutzer und als zentralen Support ausüben, gibt es auch eine Reihe an Benutzern, die bezüglich ihrer jeweils selbst genutzten PC lokaler Administrator sind. Diese lokalen Administratoren und ihre Arbeitsplatzrechner werden in erster Linie aus Gründen der IT-Sicherheit über eine entsprechende Benutzerverwaltung erfasst. Die Erfassung ist Aufgabe der Administratoren für Arbeitsplatzrechner.

3 Teil B – spezifische Regelungen

3.1 Berücksichtigte Besonderheiten des ZDF

Für alle in Ziffer 2.3 genannten Administratoren gelten generell die Rahmenbedingungen und Regelungen der Ziffern 1 und 2. Für wesentliche Teile der Informationstechnologie im ZDF, die speziell auf typische Ziele des Sendeunternehmens sowie ein eingegrenztes Aufgabenumfeld ausgerichtet sind, sind im folgenden Ausnahmeregelungen beschrieben.

Für eine strukturierte Beschreibung der nachfolgenden spezifischen Regelungen werden den IT-Systemen drei mögliche Systemtypen unterstellt:

- Sendenahe Systeme im überwiegend produktionstechnischen und sendebetrieblischen Einsatz, die durch spezielle branchenspezifische Software oder Betriebsabläufe gekennzeichnet sind,
- Arbeitsplatzsysteme, die durch eine auf eine einzige Person beschränkte Nutzung gekennzeichnet sind,
- Alle übrigen IT-Systeme.

In Bezug auf den möglichen Missbrauch personenbezogener Daten sind sendenahe Systeme und lokal administrierte Arbeitsplatzsysteme gesondert zu betrachten. Spezielle Risiken für personenbezogene Daten bestehen vor allem in netzwerkbezogenen Gefährdungen, wie etwa Software-Viren und Hackerangriffen. Auch kann die Speicherung vor Zugriff oder Manipulation zu schützender Daten (etwa brisantes Videomaterial) eine sendebezogene Aufgabenstellung sein, wodurch das zur Speicherung eingesetzte IT-System als kritisch i. S. des Datenschutzes einzustufen wäre.

Diese Sachverhalte werden im hier vorliegenden Dokument nicht vertieft behandelt, da im Einzelfall Risiken bzw. Gefährdungspotenziale und Sicherheitsaufwand aufeinander abgestimmt werden müssen. Sendenahe IT-Systeme sind im Regelfall autark, das heißt ohne Einflussmöglichkeiten auf andere Systemtypen und dort gespeicherte personenbezogene Daten.

Ebenso dürfen persönliche Arbeitsplatzsysteme durch die Ausübung lokaler Administratorenrechte keinerlei Zugang zu weiteren IT-Systemen und dort gespeicherten personenbezogenen Daten anderer Personen gewähren. Weitere Rahmenbedingungen, die diese Betrachtungsweise ermöglichen, werden in Ziffer 3.2 genannt.

3.2 Spezifische Regelungen und Einschränkungen

3.2.1 Allgemeine Regelung

Sendenah eingesetzte IT-Systeme dürfen im Regelfall nicht unmittelbar mit dem allgemeinen ZDF-Netzwerk verbunden sein (nicht an den Domänen zdf, zdf_mainz). Ausnahmen sind mit dem IT-Sicherheitsbeauftragten abzustimmen.

3.2.2 Systemadministratoren

Für Systemadministratoren gelten folgende Grundsätze:

- Berechtigungen als sogenannter "Super-Administrator" dürfen nur in solchen Fällen genutzt werden, in denen dies speziell erforderlich ist, jede andere Administratorentätigkeit muss mit eingeschränkten, der Aufgabe entsprechenden Rechten ausgeübt werden.
- Der Zugriff auf System-Accounts, die je nach System und Notwendigkeit als Notfall-Accounts dienen und die unter definierten Bedingungen verwendet werden dürfen (kein sonstiger Zugriff möglich), ist auf einen möglichst kleinen und erforderlichen Personenkreis einzuschränken.
- System-Accounts, die betriebssystem- oder applikationsbedingt erforderlich sind, können nicht durch personalisierte Accounts ersetzt werden.

Bei der Umsetzung sind innerhalb der einzelnen Teams die jeweils vorhandenen technischen, wirtschaftlichen und betrieblichen Möglichkeiten zu berücksichtigen. Hierunter fallen insbesondere die Existenz oder Nicht-Existenz von personenbezogenen Daten auf den betroffenen IT-Systemen sowie die Charakterisierung von Systemen als senderelevant bzw. sendenah.

Erweitertes Logging auf dem Großrechner (Host):

Das Security System des Großrechners protokolliert nur administrative Tätigkeiten der Administratoren. Dieses Protokoll wird täglich auf Band gesichert und im Outputmanagement System archiviert. Diese Daten können im Nachhinein nicht mehr verändert werden. Der lesende Zugriff auf diese Daten ist nur von Host-Accounts der Beschäftigten des System Management Host möglich. Im Hostbereich werden die folgenden Daten protokolliert:

- Datum
- Uhrzeit
- Host UserID (= Anmeldenamen)
- Administratives Kommando

Erweitertes Logging auf sensiblen Netzwerkkomponenten:

Auf sensiblen und sicherheitskritischen Netzwerkkomponenten (Firewalls, Router, Zugangssysteme) werden systembedingt neben den in Abschnitt 2.1.2 beschriebenen Informationen auch Änderungen an der Konfiguration des Systems protokolliert. Umfang und Dauer der Speicherung dieser Protokollierung richtet sich dabei nach den technischen Möglichkeiten und den betrieblichen Erfordernissen. Die gespeicherten Informationen sind ausschließlich den betreuenden Systemadministratoren zugänglich.

Protokollierung von Tätigkeiten auf Windows-Servern:

Auf Windows-Servern werden die in Abschnitt 2.1.2 beschriebenen Informationen über administrative Tätigkeiten nicht standardmäßig protokolliert. Um bei sicherheitskritischen Vorfällen auf entsprechende Logdaten, die die in Abschnitt 2.1.2 beschriebenen Informationen enthalten, zurückgreifen zu können und diese auch ggf. zentral zu sichern, wird ein Logging für alle Server-Benutzer aktiviert (etwa mittels einer entsprechenden Domänen-Einstellung).

Unix-Administratoren:

Auf jedem Unix-System existiert betriebsystembedingt ein zentraler System-Account (root), über den das gesamte System administrierbar ist. Aufgrund des grundsätzlichen Berechtigungskonzepts unter Unix ist es für die Unix-Systemadministratoren erforderlich, Zugang zu diesem Account zu haben.

3.2.3 Applikationsadministratoren (systemverantwortliches IT-Personal)

Mit Bezug auf die in Ziffer 2.2.1 behandelte Erfassungsstruktur und in Ziffer 2.1.1 geforderten Administratorenlisten ist eine genaue Liste mit den im ZDF eingesetzten Applikationen erforderlich.

Eine Aufstellung aller vom GB IST entwickelten bzw. betreuten Applikationen mit entsprechenden Systembeschreibungen wird im GF Planung und Realisierung geführt. Weitere Applikationen, die sendenahe Funktionen erfüllen, werden in Ziffer 3.2.5 behandelt. Bei jenen Applikationen handelt es sich in der Regel um branchenspezifische IT-Lösungen, bei denen Hardware und Software eng miteinander verbunden sind. Auch hierzu werden Applikationslisten geführt.

Applikationen, in denen personenbezogene Daten verarbeitet werden, sind gem. LDSG darüber hinaus in ein ZDF-Datenschutzregister aufgenommen und die entsprechenden Informationen für alle ZDF-Beschäftigte online einsehbar.

3.2.4 Applikationsadministratoren (in den Fachbereichen)

Die Vergabe von Berechtigungen für die Nutzung von Applikationen erfolgt i. d. R. durch IT-Personal (systemunterstütztes zentrales Antragsverfahren und Benutzerverwaltung). Differenzierte Berechtigungen für Host-Applikationen und einzelne sogenannte Client-Server-Systeme können auch dezentral in den Fachbereichen vergeben werden.

Verantwortlich für die Einhaltung der Administratoren-Reglungen sind auch hier die sogenannten IT-Sicherheitsmanager. Diese werden bei der Übergabe einer Applikation an einen Leistungsnehmer (z. B. Fachbereich im ZDF) eindeutig festgelegt. Änderungen sind vom Leistungsnehmer mitzuteilen.

Zentral verfügbar gehalten werden Informationen über die jeweils zugeordneten IT-Sicherheitsmanager in der in Ziffer 3.2.3 behandelten Applikationen-Liste. Innerhalb der im ZDF eingesetzten Standard-Kaufsoftware existieren eigene applikationsspezifische

sche Möglichkeiten zur Vergabe, Verwaltung und Dokumentation von Nutzer-Berechtigungen. Die Vergabe von differenzierten Berechtigungen auf Applikationsebene kann in diesem Fall durch Applikationsadministratoren in den jeweiligen Fachbereichen vorgenommen werden.

Im Falle der dezentralen Berechtigungsvergabe ist der Fachbereich für Folgendes verantwortlich:

- Benennung von Personen, die zur Vergabe von Berechtigungen auf Applikationsebene befugt sind,
- Festlegung eines fachbereichsinternen Antrags- und Genehmigungsverfahrens gem. Vier-Augen-Prinzip.

Liegen spezielle applikationsspezifische Regelungen im Zusammenhang mit der Vergabe von Berechtigungen vor, vgl. z. B. die Verwaltungsanordnung VwAO-149/03 für die Applikation R/3, so sind diese anzuwenden und die jeweiligen Fachbereiche für deren Einhaltung verantwortlich.

3.2.5 Administratoren für sendenahe Systeme

Sendenahe Systeme sind z. B. DPA, Harris, DVB, Websy, Teletext und die DBC Content Management Systeme (CMS).

Verschiedene lokale System-Accounts müssen aus Gründen der Betriebssicherheit über Administratorrechte verfügen. Sofern aus technischen Gründen keine Einrichtung von namentlichen Benutzern möglich ist, so gilt auch hierfür, dass die System-Accounts nur einem begrenzten Personenkreis zugänglich sein dürfen, der in entsprechenden Administratorenlisten nachvollziehbar zu dokumentieren ist.

In technisch (z. B. systemseitig) begründeten Ausnahmefällen kann bei sendenahe Client-Systemen das Antrags- und Dokumentationsverfahren entfallen. Allerdings sind auch in diesen Fällen die Personen mit Administrationsrechten schriftlich zu erfassen.

3.2.6 Administratoren für Arbeitsplatzrechner (IT-Personal)

Alle für den Einsatz an Arbeitsplätzen und unterwegs vorgesehenen PC und Laptop des ZDF sind eindeutig einer sogenannten Domäne zugeordnet (z. B. zdf_mainz). Zum Zweck der Administration werden auf den Geräten Gruppenadministrationsberechtigungen eingetragen. Mitglieder dieser Gruppen sind die professionellen IT-Beschäftigten, zu deren Aufgabenbereich die Administration und Verwaltung der Client-Endgeräte gehört.

Beantragung, Ablauf und Erneuerung der Administratorberechtigung auf Arbeitsplatzrechnern richten sich nach den Prozessen und Befristungsfestlegungen der Systemadministratoren (Beispiel für eine Administratorengruppe ist zdf_mainz\PC-Support).

3.2.7 Lokale Administratoren (Benutzer)

Anwender können unter bestimmten Voraussetzungen auf den von ihnen genutzten Arbeitsplatzrechnern lokale Administratorberechtigung erhalten. Diese Berechtigung gilt, solange sie auf dem Gerät benötigt wird, längstens jedoch bis zum Ende der Nutzungsdauer des Gerätes. Im Falle eines Geräteaustausches ist das Beantragungsverfahren erneut in Gang zu setzen. Lokale Administratoren verlieren ihre Administratorrechte demnach beim Gerätewechsel.

Folgende Vergabeumstände werden berücksichtigt:

- Es sind Softwareinstallationen an Einsatzorten vorzunehmen, an denen kein physikalischer ZDF Netzwerkzugang zur Verfügung steht.
- Hardwareanpassungen müssen an wechselnden Einsatzorten vorgenommen werden.
- Regelmäßige Softwareinstallationen, die z. B. Entwickler, Webmaster auf ihrem eigenen Arbeitsplatzrechner im Rahmen von dienstlichen Entwicklungs-, bzw. Testtätigkeiten durchführen müssen.
- Der fehlerfreie Betrieb der installierten Software benötigt zwingend administrative Berechtigungen.

4 Verpflichtungserklärung

Beschäftigte (feste Mitarbeiter/innen, freie Mitarbeiter/innen sowie Praktikant/innen) mit Administratoren-Aufgaben müssen vor Aufnahme ihrer Tätigkeit die als Anlage beige-fügte Verpflichtungserklärung abgeben. Diese wird zum Bestandteil der Personalakte bzw. Vertragsakte.

Sofern Dienstleister eigenes Personal für Administratorentätigkeiten im ZDF einsetzen, schließt das ZDF hierüber Dienstleistungsverträge ab, die Vereinbarungen zu Datenschutz und IT-Sicherheit beinhalten. Diese Vereinbarungen müssen mindestens das-selbe Maß an Verpflichtungen erzielen, wie es für ZDF-Beschäftigte gilt.

Dem IT-Sicherheitsbeauftragten und dem Datenschutzbeauftragten sind vertraglich die erforderlichen Kontrollrechte einzuräumen. Im Zweifelsfall werden Administratorentätigkeiten durch externe Dienstleister nur unter Aufsicht eines sachkundigen ZDF-Beschäftigten durchgeführt.

5 In-Kraft-Treten

Diese Regelung tritt mit sofortiger Wirkung in Kraft.