Systemverwaltung

Orientierungshilfe und Checkliste

Landesbeauftragter für den Datenschutz Niedersachsen

Allgemein

Um einen geordneten Betrieb von Informations- und Kommunikatiosnsystemen zu ermöglichen, ist ein Systemadministrator erforderlich. Personen, die mit der Systemverwaltung betraut werden, sollten folgende Aufgaben erfüllen:

- Mitarbeit bei Organisation und Planung des IuK-Technikeinsatzes
- Systemadministration
- Netzwerkverwaltung und –überwachung
- Systemoperating und Wartung
- Kontroll- und Organisations- und Betreuungsmaßnahmen zur Gewährleistung von Datenschutz und Datensicherung

Fachkunde und Zuverlässigkeit

Die Auswahl des Systemadministrators und der Vertretung erfolgt sorgfältig nach Fachkunde (EDV-Wissen, betriebsspezifische Kenntnisse) und Zuverlässigkeit (persönliche Integrität). Hierbei muß auch berücksichtigt werden, dass Aus- und Fortbildung des Systemadministrators erfolgen. Für die Übernahme von Administrationsaufgaben muß die datenverarbeitende Stelle gewährleisteten, dass dem Administrator und seinem Vertreter für eine sorgfältige Aufgabenerfüllung auch die hierfür erforderliche Zeit zur Verfügung steht.

Systemverwaltung bei Netzwerkbetriebssystemen

Viele Netzbetriebssysteme bieten die Möglichkeit, die Administratorrolle aufzuteilen und Administrationstätigkeiten an verschiedene Benutzer zu verteilen. So können z. B. unter Novell Netware 3.11 die folgenden Administratorrollen eingerichtet werden: Workgroup Manager, User Account Manager, File Server Console Operator, Print Server Operator, Print Queue Operator. Unter Windows NT können durch die gezielte Vergabe von Benutzerrechten an einzelne Benutzer oder besser an Gruppen definierte Administratorrollen geschaffen werden. Neben der Gruppe der Administratoren sind hier die Gruppen Hauptbenutzer (d.h. Administratoren mit eingeschränkten Rechten), Sicherungs-Operatoren, Druck-Operatoren, Server-Operatoren sowie Reproduktions-Operatoren zu nennen. Bei den meisten Unix-Systemen gibt es nur eine Administrationsrolle (den *Super-User* namens *root* mit der Benutzer-ID (UID) 0). Personen mit Zugang zu dieser Rolle haben die volle Kontrolle über das System. Insbesondere können sie unabhängig von Zugriffsrechten jede Datei lesen, verändern und löschen.

In jedem Fall muß die Weitergabe von Administrationsrechten an andere Benutzer sorgfältig geprüft werden und sollte nur in größeren Systemen mit mindestens 20 Benutzern erfolgen. Sie ist zu dokumentieren und so zu handhaben, dass nicht die Kontrolle über das System verloren geht.

Systemverwalter-Kennung und Passwort

Der Administrator eines Netzwerkbetriebssystems verwendet bei der Installation und späteren Verwaltung des Netzwerkes eine vordefinierte Kennung, z.B. Administrator bei Windows NT. Das Administratorkonto kann umbenannt, jedoch nicht gelöscht werden.
Das Systemverwalter-Passwort darf nur den Administratoren bekannt sein und ist geheim zu halten. Für die normale Arbeit darf das Systemverwalterpasswort nicht eingesetzt werden. Bestehen Anhaltspunkte für ein Bekanntwerden des Passwortes, ist dieses unverzüglich zu ändern.
Bei großen Netzen mit möglicherweise mehreren Administratoren ist es erforderlich, für jeden Administrator eine eigene Benutzerkennung einzurichten und diese Kennung der Gruppe der Administratoren hinzuzufügen. Die Administratorkennung ist dann nur in Notfällen zu gebrauchen.

Protokollierung
Der Administrator, der unter der Administratorkennung oder einer Kennung mit gleichen Rechten arbeitet, kann nachvollziehbar z. B. alle Programme und alle Dateien lesen und verändern und in die Zugriffsmechanismen und Ein- und Ausgabeprozesse des Betriebssystems eingreifen. Ihm obliegt außerdem die Einrichtung und Verwaltung von Benutzern, die Zugriff auf das Netzwerk haben. Zwar kann sich der Administrator bei vielen Netzwerkbetriebssystemen einzelne dieser Rechte selbst entziehen, er kann sie sich aber auch selbst wieder zuteilen. Als einziger Schutz bleibt in diesem Fall die Protokollierung von Administrationstätigkeiten. Dennoch bleibt der Administrator nur bedingt kontrollierbar. Daraus ergeben sich folgende Risiken:

- Der Administrator oder jede andere Person mit entsprechenden Rechten kann die umfassenden Berechtigungen für unlautere bzw. datenschutzrechtlich bedenkliche Zugriffe und Manipulationen der Programme oder Daten nutzen.
- Fehler des Administrators können weitreichende unerwünschte Konsequenzen haben.

Einrichtung und Löschung von Benutzern
Die Systemverwaltung richtet die Benutzer ein und legt die Systemprivilegien fest. Beim erstmaligen Zugriff eines Benutzers auf das System hat dieser das von der Systemverwaltung festgelegte Passwort zu ändern.
Die Systemverwaltung hat Benutzerkonten, die vorübergehend nicht benutzt werden, unverzüglich zu sperren. Ist davon auszugehen, dass Benutzerkonten dauerhaft oder endgültig nicht mehr benutzt werden, sind die Daten des Benutzerkontos zu sichern und das Benutzerkonto unverzüglich zu löschen.

Umgang mit Datenträgern
Datenträger sind von der Systemverwaltung grundsätzlich so aufzubewahren, dass eine unzulässige Offenbarung personenbezogener Daten ausgeschlossen ist. Alle Datenträger, auch solche, die lediglich Programmdateien enthalten, sind verschlossen aufzubewahren, so dass eine Nutzung Dritter ausgeschlossen ist. Datenträger, die vernichtet werden sollen, sind vorher physikalisch zu löschen. Die Vernichtung ist zu überwachen. Für die Durchführung der Datensicherungsmaßnahmen hat die Systemverwaltung folgende Punkte zu beachten:

- Es ist für jeden Rechner ein Protokoll der Datensicherung in Listenform anzulegen. Die Durchführung der Datensicherung ist durch Handzeichen und Datum zu bestätigen.
- Die Datensicherung ist täglich durchzuführen. Pro Wochentag sind ein oder mehrere Datenträger anzulegen. Die Datenträger, die älter als ein Jahr sind, müssen vernichtet und ersetzt werden.
- Am letzten Arbeitstag eines Monats sind Monatsdatenträger an Stelle der Tagesdatenträger zu verwenden. Die Verwendung der Monatsdatenträger in Folgejahren ist zulässig.
- Am letzten Arbeitstag des Jahres sind Jahresdatenträger an Stelle der Tagesdatenträger zu verwenden. Die Jahresdatenträger sind mindestens 10 Jahre aufzubewahren.
- Alle Datenträger und Protokolle sind außerhalb des EDV-Raumes, in dem die Server stehen, sicher aufzubewahren. Nur die am jeweiligen Tage benötigten Datenträger dürfen innerhalb des Raumes, in dem sich die Rechner befinden, aufbewahrt werden.
- Für alle Datenträger gilt, dass sie vor Diebstahl, Zerstörung, Einsichtnahme und Manipulation zu schützen sind.

Technische Arbeitsabwicklung

Bei der technischen Abwicklung von dezentralen DV-Verfahren hat die Systemverwaltung sicherzustellen, dass

- nur die zuletzt freigegebenen Programme (Revisionsstand) verwendet werden,
- nur freigegebene Programme in der Produktionsbibliothek archiviert werden,
- nachgewiesen wird, welches Programm für welche Arbeit eingesetzt wurde,
- Datenbestände eindeutig gekennzeichnet und Sicherungsmöglichkeiten ausgenutzt werden,
- durch Plausibilitätsprüfungen die größtmögliche Integrität der Daten gewährleistet ist,
- durch entsprechende Wiederanlaufroutinen Systemzusammenbrüche usw. schnell überbrückt werden können (Schutz der Verfügbarkeit),
- die Funktionsfähigkeit der Datenverarbeitungsanlage und der angeschlossenen Endgeräte jederzeit gewährleistet ist,
- die notwendigen Wartungsarbeiten erfolgen und
- Unbefugte sich nicht in den Besitz von Daten oder Datenträgern bringen können.

Sicherung des Rechnerraumes

Zum Rechnerraum haben nur die Bediensteten der Systemverwaltung Zugang. Weiteren Personen ist ein Zutritt nur in Abstimmung mit erstgenannten Personen erlaubt.Der Rechnerraum ist stets verschlossen zu halten. Die Tür zum Rechnerraum darf sich nicht mittels Generalschlüssel öffnen lassen.

Checkliste

Die folgende Checkliste soll eine Hilfestellung für der Auswahl und Kontrolle der Systemverwaltung leisten. Sie konzentriert sich auf die Gesichtspunkte des technisch-organisatorischen Datenschutzes.

Zur Beantwortung der Checklisten-Fragen wird es in der Regel ausreichen, jeweils anzukreuzen

- **Erfüllt**
- **Nicht erfüllt**
- **Trifft nicht zu.**

Diese Basisantworten können im Bedarfsfall durch kurze Erläuterungen in dem Feld Bemerkungstext ergänzt werden. Auf diese Weise liegt nach Durcharbeiten der Checkliste eine übersichtliche Aufstellung der noch zu treffenden Maßnahmen vor.

Eine beantwortete Checkliste deckt möglicherweise vorhandene Sicherheitslücken des Systems auf. Daher ist die ausgefüllte Checkliste bis zur vollständigen Beseitigung dieser Mängel entsprechend vertraulich zu behandeln!

Checkliste – Systemverwaltung

Klassifizierung der Schutzstufe Begründung der Einstufung (Extrablatt)				
Stufe A	**Stufe B**	**Stufe C**	**Stufe D**	**Stufe E**

Erläuterung:
Die einzelnen Anforderungen sind nach dem Schutzstufenkonzept (siehe Anlage) gestaffelt aufgeführt. Die Grundschutzforderungen unter der Schutzstufe A – C sind immer anzuwenden. Die unter den Schutzstufen D oder E aufgeführten Anforderungen kommen aufgrund der höheren Datenschutzsicherungsanforderung jeweils ergänzend hinzu.

1	**Systemverwaltung**	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkungen
Daten der Schutzstufe A – C:					
1.1	Bei kleineren Systemen mit weniger als 20 Teilnehmern gibt es einen Systemadministrator und mindestens eine Vertretung.				
1.2	Bei größeren Systemen mit mindestens 20 Teilnehmern ist auch die Einrichtung von weiteren Administratoren denkbar, wobei deren Anzahl der Systemgröße angepasst ist.				
1.3	Sind mehrere Administratoren vorhanden, so vertreten diese sich untereinander.				
1.4	Die Namen, die Rechte und die Verpflichtungen des Systemadministrators bzw. des Vertreters sind in einer Dienst- oder Betriebsanweisung schriftlich festgelegt worden.				
1.5	Die Zuweisung der Funktion als Systemadministrator bzw. als Vertreter ist schriftlich vorgenommen worden.				
1.6	Der Systemadministrator bzw. der Vertreter üben nicht gleichzeitig die Funktion des Datenschutzbeauftragten aus.				

1	**Systemverwaltung**	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkungen
1.7	Die Auswahl des Administrators und der Vertretung erfolgte sorgfältig nach Fachkunde (EDV-Wissen, betriebsspezifische Kenntnisse) und Zuverlässigkeit (persönliche Integrität).				
1.8	Dem Systemadministrator steht ausreichend Zeit zur Verfügung, um die ihm übertragenen Aufgaben in Absprache mit der Fachabteilung in entsprechendem Umfang wahrzunehmen.				
1.9	Der Systemadministrator bzw. der Vertreter sind auf das Datengeheimnis verpflichtet (§ 5 BDSG) bzw. darüber belehrt worden (§ 5 NDSG).				
1.10	Außer dem Systemadministrator bzw. seinem Vertreter hat keine weitere Person Zugang zur Betriebssystemebene.				
1.11	Im Notfall haben der Systemadministrator bzw. der Vertreter neben der normalen Kennung noch die Möglichkeit, sich über eine Notfall-Kennung anzumelden.				
1.12	Das Kennwort des Systemadministrators ist sicher hinterlegt (z.B. Tresor).				
1.13	Der Systemadministrator hat neben seinen administrativen Aufgaben nicht die Möglichkeit, personenbezogene Daten in den jeweiligen Anwendungen zu bearbeiten.				
1.14	Der Systemadministrator bzw. der Vertreter haben neben der besonderen Kennung (als Systemadministrator) ihre normale Benutzer-Kennung, um ihre Benutzeraufgaben durchzuführen.				
1.15	Einem Benutzer mit normalen Rechten sind keine Systemadministratorrechte eingeräumt worden.				
1.16	Alle Aktivitäten des Systemadministrators bzw. des Vertreters werden automatisiert protokolliert und regelmäßig kontrolliert.				

1	**Systemverwaltung**	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkungen
1.17	Der Einsatz von Dienstprogrammen, die bestehende Schutzmaßnahmen unterlaufen können, wird protokolliert und kontrolliert.				
1.18	Der Systemadministrator und sein Vertreter arbeiten nur dann unter der Administrator-Kennung, wenn administrative Aufgaben wahrgenommen werden.				
1.19	Es wird von den Administratoren ein manuelles „Schichtbuch“ geführt, in dem alle wichtigen Vorkommnisse aufgezeichnet werden, die nicht automatisiert protokolliert werden.				
1.20	Administrative Aufgaben dürfen nur an bestimmten Arbeitsplätzen durchgeführt werden.				
1.21	Für Verzeichnisse und Dateien mit sensiblen Inhalt sind dem Systemadministrator die Zugriffsrechte entzogen worden.				
1.22	Es wird eine Trennung zwischen normalen Betriebssystemarbeiten und Sicherheitseinstellungen am Betriebssystem vorgenommen.				
1.23	Die notwendigen Datensicherungsmaßnahmen (Aufbewahrung, Vernichtung, Löschung) werden von der Systemverwaltung umgesetzt.				
Daten der Schutzstufe E					
1.24	Der Systemadministrator und sein Vertreter haben eine gemeinsame Super-User-Kennung mit einem zweigeteilten Kennwort, von dem jedem nur eine Hälfte bekannt ist. Super-User-Funktionen können nur gemeinsam ausgeführt werden, so daß eine gegenseitige Kontrolle erfolgt.				
1.25	Es sind mindestens zwei Systemadministratoren zur Durchführung des 4-Augen-Prinzips benannt worden.				

Anhang - Schutzstufenkonzept

Personenbezogene Daten werden nach dem Grad möglicher Beeinträchtigung schutzwürdiger Belange bei Mißbrauch dieser Daten in 5 Schutzstufen untergliedert. Bei der Klassifizierung sind Datenfelder niemals einzeln zu bewerten. Die Betrachtung ist vielmehr auf die gesamte Datei, ggf. auf die DV-Anlage auszudehnen. Werden personenbezogene Daten unter einem Auswahlkriterium in eine Datei aufgenommen, das in der Datei nicht enthalten ist, so ist dieses Auswahlkriterium bei der Klassifizierung mit zu bewerten. Enthalten Dateien umfassende Angaben zu einer Person (Dossiers), so sind sie in eine höhere Schutzstufe einzuordnen, als dies nach den Einzeldaten erforderlich wäre.
Es werden folgende Schutzstufen unterschieden:

Stufe A: Frei zugängliche Daten, in die Einsicht gewährt wird, ohne daß der Einsichtnehmende ein berechtigtes Interesse geltend machen muß, z.B. Adreßbücher, Mitgliederverzeichnisse, Benutzerkataloge in Bibliotheken.

Stufe B: Personenbezogene Daten, deren Mißbrauch zwar keine besondere Beeinträchtigung erwarten läßt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse des Einsichtnehmenden gebunden ist, z.B. beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen.

Stufe C: Personenbezogene Daten, deren Mißbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann ("Ansehen"), z.B. Einkommen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten.

Stufe D: Personenbezogene Daten, deren Mißbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann ("Existenz"), z.B. Unterbringung in Anstalten, Straffälligkeit, Ordnungswidrigkeiten schwerwiegender Art, dienstliche Beurteilungen, psychologisch-medizinische Untersuchungsergebnisse, Schulden, Pfändungen, Konkurse.

Stufe E: Daten, deren Mißbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann, z.B. Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können.

Falls die Sensitivität nicht bekannt ist, ist von der höchsten Sensitivitätsstufe auszugehen. Denkbar ist auch, daß der Schutz empfindlicher Firmendaten ohne Personenbezug die Einstufung bestimmt.