Dienstanweisung Wartung von IT-Systemen und -Anwendungen durch Fremdfirmen (DA IT-Wartung)

Vom 11.05.2022

1. Gegenstand 2

2. Geltungsbereich 2

3. Grundsätzliche Aussagen 2

4. Organisatorische Rahmenbedingungen 3

4.1. Verantwortlichkeiten 3
4.2 Zugelassenes Wartungspersonal 3
4.3 Datenschutz und Informationssicherheit 4
4.4 Kontrollmaßnahmen 4
4.5 Informationspflicht 4

5. Sicherheitsanforderungen 4

5.1 Authentifizierung 5
5.2 Protokollierung 5
5.3 Beaufsichtigung 5
5.4 Zugriffskontrolle 5
5.5 Dokumentation 6
5.6 Funktionstest 6
5.7 Datenübertragung 6
5.8 Datenträgertransport 6

6. Zusätzliche Regelungen für die Fernwartung 6

6.1 Technische Realisierung 7
6.1.1 Betrieb 7
6.1.2 Dokumentation 7
6.1.3 Änderung 8
6.2 Sicherheitsanforderungen 8
6.2.1 Zugangs- und Verbindungskontrolle 8
6.2.2 Authentifizierung 8
6.2.3 Übertragungsschutz 8

7. Personalrat 9

8. Schlussbestimmung 9

9. Inkrafttreten 9

1. Gegenstand

Im Westdeutschen Rundfunk steigt durch den wachsenden Einsatz von immer komplexer werdenden IT-Systemen und Anwendungen der Bedarf, diese durch Fremdfirmen warten zu lassen. Sowohl aus Kostengründen als auch aus Zeitgründen wird in diesen Fällen zur Systempflege und Fehlerbehebung vermehrt eine Fernwartung betrieben. Der Zugriff fremder Personen auf Ressourcen des WDR muss jedoch aus Sicht des Datenschutzes und der Informationssicherheit definierte Anforderungen erfüllen.

Diese Dienstanweisung legt die Verantwortlichkeiten bei der Wartung von IT-Systemen und Anwendungen für die Beschäftigten des WDR sowie für Fremdfirmen, deren Personal für den WDR tätig ist, fest. Zusätzlich werden die Anforderungen an die jeweiligen Wartungskonzepte des WDR beschrieben. Wartung im Sinne dieser Dienstanweisung umfasst die Wartung, Inspektion und Instandsetzung sowohl vor Ort als auch mittels Fernzugriff.

2. Geltungsbereich

Diese Dienstanweisung gilt für alle Bereiche im Westdeutschen Rundfunk und ist in allen IT-Planungs- und IT-Betriebskonzepten zu berücksichtigen.

Sofern IT-Systeme oder Anwendungen des WDR von Fremdfirmen gewartet werden, ist durch die anfordernde Stelle zu veranlassen, dass die Fremdfirmen vertraglich zur Einhaltung der Anforderungen aus dieser Dienstanweisung sowie zu Vertragsstrafen im Falle von Verstößen verpflichtet werden.

Können Anforderungen in dieser Dienstanweisung aus technischen oder betrieblichen Gründen nicht umgesetzt werden, sind die Ausnahmen zu begründen und von der Leitung der jeweils zuständigen Direktion zu genehmigen. Die begründeten Abweichungen sind im zugehörigen IT-Betriebskonzept zu dokumentieren. Außerdem sind die beauftragte Person für Informationssicherheit im WDR (Informationssicherheitsbeauftragte:r) sowie die beauftragte Person für betrieblichen Datenschutz (Datenschutzbeauftragte:r) zu informieren.

3. Grundsätzliche Aussagen

Technisch und organisatorisch ist sicherzustellen, dass eine Wartung oder Fernwartung nur mit dem Einverständnis und auf konkrete Weisung des WDR erfolgen kann.

Generell müssen auch für Daten, die über Wartungsverbindungen übertragen werden, mindestens die im lokalen Netz geltenden Sicherheitsanforderungen der

technisch organisatorischen Maßnahmen beispielsweise bezüglich Vertraulichkeit, Integrität und Verfügbarkeit (Artikel 32 Absatz 1 EU-Datenschutzgrundverordnung) durchsetzbar sein. Zusätzlich müssen Berechtigungen und Einschränkungen, die für lokale Ressourcen festgelegt wurden, auch für externe beziehungsweise entfernte Zugriffe durchgesetzt werden.

Bei jeder Fernwartungsmaßnahme ist vorher zu klären, ob und inwieweit mit personenbezogenen Daten gearbeitet werden muss. Ein Zugriff des Wartungspersonals auf personenbezogene Daten darf nur erfolgen, wenn sich ohne Kenntnis der Daten der Fehler des IT-Systems nicht beheben lässt. In Zweifelsfällen ist die beauftragte Person für betrieblichen Datenschutz im WDR einzuschalten.

4. Organisatorische Rahmenbedingungen

4.1. Verantwortlichkeiten

Die Wartung wird von den Informationsverantwortlichen initiiert beziehungsweise von den betreffenden Personen mit Informationstreuhänderschaft (Informationstreuhänder:innen). Sie sind für die Kontrolle der durchgeführten Arbeiten und die (zeitliche) Dokumentation in den Betriebshandbüchern verantwortlich. Die Dokumentation der durchgeführten Arbeiten wird durch die ausführende Firma im Rahmen eines Wartungsprotokolls erstellt. Ist im Rahmen einer Wartung der Zugriff auf WDR-spezifische Daten oder deren Transport per Datenübertragung oder Datenträger erforderlich, muss eine entsprechende Genehmigung der zuständigen informationsverantwortlichen Person vorliegen. Für die Kontrolle des Datentransports ist die betreffende Personen mit Informationstreuhänderschaft zuständig und verantwortlich.

In einem Wartungsvertrag sind klare Richtlinien hinsichtlich der Abgrenzung der Kompetenzen und Pflichten zwischen dem Wartungspersonal und dem WDR zu treffen. Art und Umfang der Wartung (Hard- und Software) sowie der Dokumentation sind schriftlich festzulegen. In den Fällen, in denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, ist ein Auftragsverarbeitungsvertrag zu schließen.

4.2 Zugelassenes Wartungspersonal

Der Kreis des autorisierten Wartungspersonals ist schriftlich festzulegen. Die erteilten Zugangs- und Zugriffsberechtigungen sind im Rahmen der IT-Betriebskonzepte zu dokumentieren und bei Änderungen fortzuschreiben. Eine interne Weitergabe von Zugangs- oder Zugriffsberechtigungen ohne vorherige Zustimmung der betreffenden Informationsverantwortlichen beziehungsweise der betreffenden Personen mit Informationstreuhänderschaft, ist nicht zulässig. Die Zustimmung ist zu dokumentieren. Ohne zuverlässige Identifikation dürfen keine Wartungsarbeiten beginnen.

4.3 Datenschutz und Informationssicherheit

Die Wartungsfirmen setzen bei der Verarbeitung personenbezogener Daten ausschließlich Personal ein, das auf das Datengeheimnis und zur Verschwiegenheit verpflichtet worden ist. Die Pflicht zur Verschwiegenheit gilt für alle internen Angelegenheiten und Vorgänge, die dem Wartungspersonal im Rahmen ihrer vertraglichen Tätigkeiten bekannt werden. Diese Verpflichtung gilt auch nach Beendigung der Tätigkeit der Wartungsfirmen fort.

Wartungsfirmen und ihr Personal, die Wartungsarbeiten an WDR-Systemen durchführen, müssen ausdrücklich auf die im WDR geltenden Bestimmungen zur Informationssicherheit und zum Datenschutz hingewiesen werden.

Da beim WDR schutzwürdige Anlagen und Einrichtungen bestehen beziehungsweise betrieben werden, ist gegebenenfalls eine Sicherheitsüberprüfung des eingesetzten Wartungspersonals erforderlich.

4.4 Kontrollmaßnahmen

Eine Überprüfung vorhandener Wartungskonzepte (zum Beispiel in der Betriebsdokumentation) wird in der Regel in Abständen von drei Jahren von den jeweils zuständigen Bereichs-Informationssicherheitsbeauftragten veranlasst. Die beauftragte Person für betrieblichen Datenschutz im WDR ist hierüber zu informieren. Eine Überprüfung vorhandener Informationsübertragungseinrichtungen wird in unregelmäßigen Abständen von der beauftragten Person für Informationssicherheit im WDR veranlasst.

4.5 Informationspflicht

Die Bereichs-Informationssicherheitsbeauftragten fordern von den Informationsverantwortlichen und den Personen mit Informationstreuhänderschaft in unregelmäßigen Abständen, mindestens einmal im Jahr, die Bestätigung der Kenntnisnahme dieser Dienstanweisung und der zugehörigen Dokumentation.

5. Sicherheitsanforderungen

Technisch und organisatorisch ist sicherzustellen, dass eine Wartung oder Fernwartung nur mit dem Einverständnis der Informationsverantwortlichen erfolgen kann. Unter den für Wartungsarbeiten eingerichteten Nutzerkennungen dürfen keine Anwenderprogramme gestartet werden, die nicht zum Wartungsumfang gehören. Der Wartungsvorgang und die zu wartenden IT-Systeme und Anwendungen einschließlich der verwendeten Kommunikationsverbindungen müssen folgenden Sicherheitsanforderungen genügen:

5.1 Authentifizierung

Das externe Wartungspersonal muss sich zu Beginn der Wartung authentifizieren. Es sind hierzu eigens für sie eingerichtete Nutzerkennungen zu verwenden, unter denen die Wartungsarbeiten durchgeführt werden.

Alle von dem Wartungspersonal verwendeten Passwörter sind unmittelbar nach Ablauf des Wartungsvertrags von den zuständigen IT administrierenden Personen (IT-Administratoren:innen) zu ändern.

5.2 Protokollierung

Die Durchführung der Wartung ist auf dem zu wartenden IT-System und auf der Kommunikationseinrichtung revisionssicher (s. Informationssicherheitsordnung Anlage 1) zu protokollieren.

Die Protokolle sind stichprobenartig von den betreffenden Personen mit Informationstreuhänderschaft oder den von ihnen benannten IT administrierenden Personen zu überprüfen und zur Beweissicherung mindestens ein Jahr aufzubewahren. Nach Abschluss der Arbeiten sind diese Daten oder Programme nach Regierungsrichtlinien (zum Beispiel DoD 5220.22-M) zu löschen.

5.3 Beaufsichtigung

Wartungspersonal ist grundsätzlich nicht unbeaufsichtigt zu lassen.

Im Falle einer Ausnahme gemäß Ziffer 2 (Geltungsbereich) muss das externe Wartungspersonal persönlich zur Wartung beziehungsweise Störungsbehebung legitimiert sein (zum Beispiel per Fax oder E-Mail) und in die Sicherheitsbestimmungen des WDR eingewiesen sowie nachweislich auf das Datengeheimnis verpflichtet worden sein. Beginn und Ende der Wartungstätigkeiten sind dem WDR unverzüglich anzuzeigen. Die Tätigkeiten des Wartungspersonals sind seitens des WDR stichprobenartig zu überprüfen.

5.4 Zugriffskontrolle

Die dem Wartungspersonal eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken.

Das Wartungspersonal darf nur auf die Daten und Verzeichnisse Zugriff haben, die aktuell von der Wartung betroffen sind. Die zu wartenden Systeme sind vor Beginn einer Wartung von allen anderen Netzwerken, die für den aktuellen Betrieb und die Wartung nicht erforderlich sind, zu trennen.

5.5 Dokumentation

Alle Aktivitäten eines Wartungsvorgangs sind zu dokumentieren (Anlass beziehungsweise Fehlerbeschreibung, Umfang, Ergebnisse, Beginn/Ende der Arbeiten, Name der Wartungsperson). Die betreffenden Personen mit Informationstreuhänderschaft oder die von ihnen benannten IT administrierenden Personen sind über die erfolgten Wartungstätigkeiten zu informieren.

5.6 Funktionstest

Im Anschluss an die Wartungs- oder Reparaturarbeiten ist die ordnungsgemäße Funktion der gewarteten Anlagen durch die betreffenden Personen mit Informationstreuhänderschaft oder die von ihnen benannten IT administrierenden Personen zu überprüfen. Insbesondere die Rücknahme der für Testzwecke vorgenommenen Eingriffe ist zu kontrollieren.

5.7 Datenübertragung

Das Wartungspersonal hat sicherzustellen, dass nur Datenträger und IT-Systeme (bspw. Wartungs-Notebook, Fernwartungszentrale) verwendet werden und Daten übertragen werden, die frei von Schadsoftware sind.

5.8 Datenträgertransport

Beim Versand beziehungsweise Transport von Datenträgern mit WDR-spezifischen Daten für Wartungszwecke ist eine der Vertraulichkeit angemessene Versandart zu wählen.

6. Zusätzliche Regelungen für die Fernwartung

Die durch eine Fernwartung entstehenden Risiken können folgendermaßen zusammengefasst werden:

Ein Wartungszugang schafft von einem externen Rechner aus eine Zugriffsmöglichkeit auf das lokale Netz. Hierbei kann der WDR nur begrenzt kontrollieren, durch welche Person tatsächlich die Wartung durchgeführt wird, welche Sicherungsmaßnahmen bei der Wartungsfirma getroffen worden sind und welche Daten übertragen werden. Die für die Wartungsverbindung genutzten Medien können häufig nicht durch den WDR vollständig kontrolliert werden.

Aus diesen Gründen ergeben sich besondere Anforderungen an die Absicherung der Kommunikation, die Authentifizierung des Wartungspersonals und die Revisionsfähigkeit des Wartungsvorgangs.

6.1 Technische Realisierung

Durch die betreffenden Personen mit Informationstreuhänderschaft veranlasst, sind alle anderen ablauffähigen Programme auf den IT-Systemen durch geeignete Zugriffsschutzmechanismen zu schützen, damit das Fernwartungspersonal nicht unkontrolliert auf Dateien zugreifen kann. Die technische Realisierung des Fernwartungszugangs ist im IT-Betriebskonzept der Anwendung beziehungsweise des IT-Systems zu beschreiben. Eventuelle Anforderungen aus dem zugehörigen Sicherheitskonzept sind dabei zu berücksichtigen.

Im Folgenden werden hierzu wesentliche, im IT-Betriebskonzept zu konkretisierende Aspekte aufgeführt.

6.1.1 Betrieb

Jede Informationsübertragung zwischen externen Stellen und dem WDR-Netz ist über eine zentrale Kommunikationseinrichtung vorzunehmen (zum Beispiel Terminalserver, VPN).

Folgende Aspekte sind im IT-Betriebskonzept zu dokumentieren:

- Mögliche interne und externe Zugangspunkte (zum Beispiel Firmennetz, Homeoffice)
- Zugelassene Kommunikationsmedien (Festnetz, Mobiltelefon, Internet)
- Authentifizierungsverfahren
- Freigegebene Hard- und Softwareprodukte
- Zu verwendende Dienste und Zugangsprotokolle
- Über den Zugang erreichbare Teilnetze und Ressourcen
- Einbindung des Zugangs in das Firewall-Konzept des WDR
- Zugangsberechtigte Personen

Die Kommunikationseinrichtung ist nur in der bestätigten und dokumentierten Installation und Konfiguration zu betreiben. Berechtigtes WDR-Personal ist, sofern notwendig, in die Nutzung der Kommunikationsverbindung einzuweisen (Schulung, Bedienungsanleitung, Sicherheitshinweise).

6.1.2 Dokumentation

Die Installation und Konfiguration der jeweiligen Informationsübertragungseinrichtung ist von der zuständigen Organisationseinheit revisionssicher zu dokumentieren

(Veränderungen müssen jederzeit nachvollzogen werden können). Die Dokumentation ist so aufzubewahren, dass Unbefugte keinen Zugriff haben.

6.1.3 Änderung

Aus betrieblichen Gründen notwendige Konfigurationsänderungen dürfen nur in Abstimmung mit der zuständigen Organisationseinheit ausgeführt werden. Die Änderungen sind zu dokumentieren und die jeweiligen Bereichs-Informationssicherheitsbeauftragten sowie die Informationsverantwortlichen zu informieren.

6.2 Sicherheitsanforderungen

Der Wartungsvorgang und die zu wartenden IT-Systeme und Anwendungen einschließlich der verwendeten Kommunikationsverbindungen müssen folgenden Sicherheitsanforderungen genügen:

6.2.1 Zugangs- und Verbindungskontrolle

Der Aufbau der Verbindung für eine Fernwartung darf nur über die zentralen Kommunikationseinrichtungen des WDR erfolgen.

Der Zugang ist nur für den Zeitraum der Fernwartung zu nutzen und bei Nichtbenutzung gegebenenfalls zu deaktivieren. Er ist durch geeignete Maßnahmen vor unautorisiertem Zugriff zu schützen (beispielsweise mittels Zwei-Faktor-Authentifizierung).

Die Beendigung der Verbindung muss sowohl durch die Fremdfirma, die eine Wartung durchführt, als auch jederzeit durch den WDR möglich sein.

6.2.2 Authentifizierung

Für jede Verbindungsaufnahme ist immer eine Authentifizierung des Wartungspersonals über die im IT-Betriebskonzept definierten Mechanismen durchzuführen. Hierzu ist auf dem jeweils zu administrierenden IT-System eine gesonderte Kennung zu nutzen. Dabei ist auf eine dem jeweiligen Schutzbedarf angemessene Authentifizierung zu achten. Müssen aus technischen Gründen Passwörter unverschlüsselt über eine unsichere Verbindung übertragen werden, sind Einmalpasswörter zu verwenden.

6.2.3 Übertragungsschutz

Zum Schutz der zu übertragenden Daten sind für die Kommunikationsverbindungen dem jeweiligen Schutzbedarf angemessene und hinreichend sichere Verfahren (zum Beispiel Verschlüsselung) anzuwenden. Die Übertragung von Daten aus IT-Systemen des WDR nach extern ist nur in Ausnahmefällen (zum Beispiel an eine Fernwartungszentrale) bei gleichzeitiger Protokollierung zulässig.

7. Personalrat

Die gesetzlichen Beteiligungsrechte des Personalrats werden durch diese Grundsätze nicht berührt.

8. Schlussbestimmung

Spezielle Rechtsvorschriften zum Datenschutz und zur Informationssicherheit für bestimmte Bereiche gehen den Bestimmungen dieser Dienstanweisung vor.

9. Inkrafttreten

Diese Dienstanweisung tritt zum 01.06.2022 in Kraft und ersetzt die Dienstanweisung IT-Wartung vom 22.10.2020.

Köln, 11.05.2022
gez. Tom Buhrow
Intendant