

Fernwartung

ZDF IT-Sicherheitsstandard

Version: 1.0
Status: Final
Datum: 27.07.2011



Inhaltsverzeichnis

1	EINLEITUNG	3
1.1	VERSIONSHISTORIE	3
1.2	ZIELSETZUNG	3
1.3	DEFINITION	3
1.4	ADRESSATENKREIS.....	4
1.5	GÜLTIGKEIT	4
2	ALLGEMEINE ANFORDERUNGEN.....	4
3	ORGANISATORISCHE ANFORDERUNGEN.....	4
3.1	VERANTWORTLICHKEITEN	4
3.2	WARTUNGSPERSONAL.....	5
4	SICHERHEITSTECHNISCHE ANFORDERUNGEN	5
4.1	AUTHENTIFIZIERUNG.....	5
4.2	VERSCHLÜSSELUNG	5
4.3	PROTOKOLLIERUNG.....	5
4.4	DATENÜBERTRAGUNG.....	6
4.5	DOKUMENTATION	6
4.6	ZUGANGSKONTROLLE	6
4.7	BEAUFSICHTIGUNG.....	6
4.8	FUNKTIONSTEST	6



Fernwartung

ZDF IT-Sicherheitsstandard

1 Einleitung

1.1 Versionshistorie

Stand	Version	Verfasser
Draft	0.1-0.4	Joachim Seifert (RBT)
	0.7	Claus Bayer
Final	1.0	Claus Bayer

1.2 Zielsetzung

Der Sicherheitsstandard Fernwartung beschreibt Maßnahmen, die unternehmensweit bei der Planung und Durchführung von Fernwartungszugriffen einzuhalten sind. In diesem Dokument werden die sicherheitstechnischen Mindestanforderungen beschrieben. Dabei sind die "Regelungen für die Administratoren der informationstechnischen Systeme" (Administratorenrichtlinie) die "Sicherheitshinweise für Administratoren im ZDF" sowie die „Nutzung der IT-Endgeräte im ZDF“ in den jeweils geltenden Fassungen zu beachten.

Diese Sicherheitshinweise basieren auf den Vorgaben des IT-Grundschutzhandbuchs des Bundesamts für Sicherheit in der Informationstechnologie (BSI).

Die Umsetzung bzw. Einhaltung der entsprechenden Maßnahmen ist in der Projektdokumentation gemäß Projektmanagementrichtlinie (VwAO-170/07), bzw. in der entsprechenden Betriebsdokumentation zu dokumentieren. Produktions- oder betriebsbedingte Abweichungen von diesem Standard sind zu begründen und ebenfalls zu dokumentieren. Sicherheitsrelevante Abweichungen müssen mit dem IT-Sicherheitsbeauftragten abgestimmt werden.

1.3 Definition

Unter dem Begriff „Fernwartung“, im Sinne dieses IT-Sicherheitsstandards, ist der Fernzugriff von im Auftrag für das ZDF tätigen Dritten auf IT- und fernsehtechnischen Produktions- und Sendesystemen zum Zwecke der Wartung zu verstehen.



1.4 Adressatenkreis

- IT-Sicherheitsmanager
- Informationstreuhand
- Im Auftrag des ZDF tätige Dritte
- Administratoren
- Anwender

1.5 Gültigkeit

Dieser Standard wurde gemäß dem IT-Sicherheitskonzept des ZDF am 25.03.2011 durch den Produktionsdirektor des ZDF bestätigt und durch den IT-Sicherheitsbeauftragten in Kraft gesetzt. Dieser Sicherheitsstandard bleibt bis zu seinem Widerruf uneingeschränkt gültig.

2 Allgemeine Anforderungen

Bedingt durch den vermehrten Einsatz komplexer IT-Unterstützung im Bürokommunikations- als auch Produktionsumfeld steigt der Bedarf, diese durch Dritte (z.B. Hersteller oder externe Wartungsfirma) zu warten bzw. bei Störungen, Fehler beseitigen zu lassen. Sowohl aus Gründen der Reaktionszeit, als auch aus Kostengründen wird in diesen Fällen zur Systempflege und/oder Fehlerbehebung vermehrt auf Fernwartung zurückgegriffen.

Während der Fernwartung wird ein Fernzugriff seitens der Wartungsfirma (Auftragnehmer) auf das zu wartende IT-System initiiert. Mit solchen Fernzugriffen durch fremdes Wartungspersonal gehen grundsätzlich die bereits im ZDF IT-Sicherheitsstandard für „Remote Access“ beschriebenen Gefährdungen einher. Daher sind im Rahmen der Fernwartung die Anforderungen des IT-Sicherheitsstandards „Remote Access“ zu beachten, bzw. geeignete Remote-Access-Verfahren des ZDF zu verwenden, welche diese Anforderungen erfüllen.

Darüber hinausgehende, zusätzliche Sicherheitsanforderungen an Fernwartung werden im Folgenden beschrieben.

3 Organisatorische Anforderungen

3.1 Verantwortlichkeiten

Die Fernwartung wird grundsätzlich durch das ZDF (Informationstreuhand, Informationsverantwortlicher) beauftragt. Dabei sind Art, Vorgehensweisen und Umfang der Fernwartung, involvierte Systeme sowie die Abgrenzung der Kompetenzen und Pflichten zwischen der Wartungsfirma und dem ZDF vertraglich zu regeln. Die Beauftragung von Sub-Unternehmen durch die Wartungsfirma ohne Rücksprache mit dem ZDF sollte vertraglich ausgeschlossen werden.

Die technische Bereitstellung des Fernwartungszugangs erfolgt durch den GB IST.



3.2 Wartungspersonal

Der Auftragsnehmer setzt zur Durchführung der Fernwartung nur autorisiertes Fachpersonal ein, das zur Verschwiegenheit verpflichtet worden ist. Die Pflicht zur Verschwiegenheit gilt für alle internen Angelegenheiten und Vorgänge, die dem vom Auftragnehmer eingesetzten Wartungspersonal im Rahmen ihrer vertraglichen Tätigkeiten bekannt werden. Diese Verpflichtung gilt auch nach Beendigung der Tätigkeit für den Auftragnehmer fort. Weiterhin ist festzulegen, dass Daten (z.B. Protokolldateien, Speicherauszüge, etc.), die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden. Eine Weitergabe der im Rahmen der Fernwartung anfallenden Daten an Dritte ist grundsätzlich untersagt und muss im Einzelfall durch das ZDF genehmigt werden.

Die externe Wartungsfirma und das Personal, das die Wartungsarbeiten durchführt, muss auf die im ZDF geltenden Bestimmungen zur IT-Sicherheit durch den Informationstreuhänder hingewiesen werden.

4 Sicherheitstechnische Anforderungen

Technisch und organisatorisch ist sicherzustellen, dass eine Wartung nur mit dem Einverständnis des ZDF (Informationsverantwortlicher, Informationstreuhänder) erfolgt.

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

4.1 Art der Kommunikationsverbindung

Fernwartungszugriffe sind über eine Presentation-Lösung zu bevorzugen. Wenn der Fernwartungszugriff nicht über die bevorzugte Lösung realisiert werden kann, ist vor Einführung der entsprechenden Verbindungsmöglichkeit eine Risikobetrachtung durchzuführen.

4.2 Authentifizierung

Der Einsatz von starken Authentifizierungsmechanismen (z.B. 2-Faktor-Authentifizierung mit Besitz und Wissen) sind an der Kommunikationseinrichtung (Sicherheit Gateway) anzuwenden. Danach muss sich das externe Wartungspersonal am eigentlichen IT-System authentifizieren. Es hat hierzu eigens für sie eingerichtete Nutzerkennungen zu verwenden, unter der die Wartungsarbeiten durchgeführt werden.

4.3 Verschlüsselung

Wird die Verbindung über Fremdnetze hergestellt, muss die gesamte Datenübertragung verschlüsselt erfolgen. Ein geeignetes Verschlüsselungsverfahren ist zu wählen. Dabei ist die technische Richtlinie BSI TR-02102 in der jeweils aktuellen Version zu beachten.

4.4 Protokollierung

Die Durchführung der Fernwartung ist auf dem zu wartenden IT-System, sowie auf dem Sicherheit Gateway zu protokollieren und auszuwerten. Der Umfang der Protokollierung hängt vom Schutzbedarf des zu wartenden IT-Systems ab. Zu beachten sind ferner die Vorgaben der „Regelung für die Administratoren der informationstechnischen Systeme des ZDF, Absatz 2.1.2“ für die Protokollierung administrativer Zugriffe.

Die Protokollierung darf vom Auftragnehmer nicht abgeschaltet oder manipuliert werden.



4.5 Datenübertragung

Notwendige Datenübertragungen zu Zwecken der Fernwartung müssen in hinreichend verschlüsselter Form erfolgen. Eine Übertragung von Daten an die Fernwartungsstelle darf nur mit Zustimmung durch den Informationsverantwortlichen geschehen. Werden während der Wartung Daten oder Programme auf dem zu wartenden IT-System abgelegt, müssen diese deutlich erkennbar und durch den Informationstreuhänder jederzeit nachvollziehbar sein.

4.6 Dokumentation

Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Anlass bzw. Fehlerbeschreibung, Umfang, Ergebnisse, Zeitpunkt, Name des/der Wartungstechnikers/in).

4.7 Zugangskontrolle

Für die Fernwartung sind die Zugriffsmöglichkeiten auf das minimal Notwendige zu beschränken, die für die Wartung/Fehlerbehebung unbedingt erforderlich sind. Das Wartungspersonal darf nur auf die Daten und Verzeichnisse Zugriff haben, die aktuell von der Wartung betroffen sind. Der Zugriff auf das IT-System ist grundsätzlich nur für den Zeitraum der Fernwartung freizugeben und bei Nichtbenutzung zu deaktivieren. Ausnahmen sind entsprechend zu begründen und in den vertraglichen Regelungen zur Fernwartung zu dokumentieren.

Die Anzahl von fehlerhaften Anmeldeversuchen ist zu begrenzen.

4.8 Beaufsichtigung

Soweit möglich sind alle Aktivitäten im Rahmen der Fernwartung in geeigneter Weise zu beaufsichtigen. Im Zweifelsfall muss eine Möglichkeit bestehen die Aktivitäten seitens des ZDF jederzeit abubrechen. Eine Beendigung der Wartungstätigkeit (Fernwartungszugang) muss sowohl durch die externe Wartungsfirma, als auch durch das ZDF möglich sein.

4.9 Funktionstest

Nach Abschluss der Wartungs- oder Reparaturarbeiten ist die ordnungsgemäße Funktion des gewarteten Systems durch den Informationsverantwortlichen bzw. Informationstreuhänder in Form einer Abnahme zu überprüfen.