

Remote Access

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	4
1.4	ADRESSATENKREIS.....	4
1.5	GÜLTIGKEIT	4
2	ALLGEMEINE ANFORDERUNGEN.....	5
3	ORGANISATORISCHE ANFORDERUNGEN.....	5
3.1	BEREITSTELLUNG	5
3.2	EINRICHTUNG.....	5
3.3	DOKUMENTATION	6
3.4	VERHALTEN BEI STÖRUNGEN UND SICHERHEITSVORFÄLLEN	6
3.5	SCHULUNGEN/UNTERWEISUNGEN	6
4	SICHERHEITSTECHNISCHE ANFORDERUNGEN	7
4.1	IT-ENDGERÄTE	7
4.2	VERSCHLÜSSELUNG	7
4.3	AUTHENTIFIZIERUNG.....	7
4.4	ZUGANGS- UND ZUGRIFFSKONTROLLE	7
4.5	PROTOKOLLIERUNG.....	7



Remote Access

ZDF IT-Sicherheitsstandard

1 Einleitung

1.1 Versionshistorie

Stand	Version	Verfasser
Draft	0.1	Joachim Seifert (RBT)
	0.3-0.7	Claus Bayer
Final	1.0	Claus Bayer

1.2 Zielsetzung

Der Sicherheitsstandard Remote Access beschreibt Maßnahmen, die unternehmensweit bei der Planung, Einrichtung und Betrieb von Remote Access Lösungen für ZDF-Mitarbeiter und im Auftrag des ZDF tätigen Dritten (im Folgenden kurz RAS-Berechtigte) 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) 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 „Remote Access“ im Sinne dieses IT-Sicherheitsstandards versteht man den „entfernten Zugriff“ von RAS-Berechtigten auf Dienste und Ressourcen im geschützten, lokalen Netzwerk des ZDF im Rahmen der dienstlichen Aufgabenerfüllung.

Prinzipiell können folgende drei Arten des Remote Access unterschieden werden:

- 1) Direkt:
Die Verbindung wird direkt zwischen einem Endgerät und dem lokalen ZDF-Netz aufgebaut (Bsp.: VPN oder Dial-In). Diese Variante wird typischerweise eingesetzt, wenn ein mobiler Benutzer von unterwegs über ein fremdes Netz (z.B. Internet oder PSTN) eine unmittelbare Verbindung zum lokalen ZDF-Netz aufbaut.
- 2) Präsentationsebene:
Der eigentliche Fernzugriff erfolgt über ein externes Netz ausschließlich auf der Präsentationsebene. Alle Daten verbleiben im geschützten, lokalen Netz des ZDF. Diese Variante kommt typischerweise zum Einsatz, wenn lediglich eine Anwendung im lokalen Netz aus der Ferne bedient werden soll. Beispiel: Citrix oder Remote Desktop.
- 3) Webbasiert:
Hier erfolgt in der Regel ein Zugriff aus dem Internet mittels eines Webbrowsers auf eine interne Webanwendung des Unternehmens über ein speziell dafür vorgesehenes Sicherheitsgateway, welches die http¹-Zugriffe aus dem externen Netz ins geschützte, lokale Netz vermittelt.

Mit dem Begriff „Remote Access“ im Sinne dieses Standards soll somit explizit keine spezielle technische Umsetzung verbunden werden, sondern als Überbegriff dafür betrachtet werden.

1.4 Adressatenkreis

- IT-Sicherheitsmanager
- Informationstrehänder
- 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.

¹ http – Hypertext Transfer Protocol



2 Allgemeine Anforderungen

Der Fernzugriff (Remote Access) auf lokale Ressourcen über moderne Kommunikationsnetze ermöglicht einerseits eine erhebliche Arbeitserleichterung andererseits stellt diese Möglichkeit des entfernten Zugriffs auf das ZDF-Netz ein großes Risiko für das Unternehmen dar.

Primär sind folgende Gefährdungen zu nennen und im Weiteren zu betrachten:

- Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
- Verwendung unsicherer Endgeräte
- Verwendung unsicherer Protokolle
- Unerwünschte Kommunikationsverbindungen
- Unzureichende Kenntnis über Regelungen
- Ungeeignete Nutzung von Authentisierungsdiensten
- Ungeeigneter Umgang mit Passwörtern

Um diesen Gefährdungen begegnen zu können, ist der Einsatz angemessener Sicherheitsmaßnahmen und die Auswahl der mit Blick auf die Gefährdungen geeignetsten Remote-Access-Variante nötig.

In den weiteren Kapiteln werden die Anforderungen an sichere Remote-Access-Lösungen beschrieben.

3 Organisatorische Anforderungen

3.1 Bereitstellung

Die technische Bereitstellung von Remote Access Lösungen im ZDF erfolgt in Übereinstimmung mit der OrgAO-PrD-09/05 ausschließlich durch den GB IST, welcher als Informationstreuhandler auftritt. RAS-Verbindungen erfolgen immer über dedizierte Gateways. Die einzusetzenden RAS-/Sicherheit Gateways sind immer durch geeignete technische Maßnahmen (wie z.B. Firewalls) vor unberechtigten Zugriffen zu schützen. Weiterhin sind bei der Planung von RAS-/Sicherheit Gateways und der zu verwendenden IT-Endgeräte Anforderungen zutreffender ZDF-Standards (z.B. allgem. Server, Client) entsprechend zu berücksichtigen.

Mittels Remote-Access ist primär der Zugriff auf Ressourcen, Dienste oder Anwendungen des Bürokommunikationsnetzwerkes des ZDF erlaubt. Für Ressourcen, Dienste oder Anwendungen mit hohem oder sehr hohem Schutzbedarf, muss vorab eine gesonderte Risikobetrachtung durchgeführt werden.

3.2 Einrichtung

Die Einrichtung eines RAS-Zugriffs auf lokale Ressourcen, Dienste oder Anwendungen des ZDF darf nur in Abstimmung mit dem entsprechenden Informationsverantwortlichen erfolgen. Hier ist immer mit Blick auf den Schutzbedarf die geeignetste Remote-Access-Variante in Kombination mit angemessenen Sicherheitsmaßnahmen zu wählen.



Remote Access auf dienstlich benötigte Ressourcen, Dienste oder Anwendungen samt zugehöriger Zugangs- und Zugriffsberechtigungen sind verbindlich durch Beantragung zu klären und zentral zu dokumentieren. Im Rahmen des Systemzugangs sind immer die gültigen IT-Sicherheitsstandards des ZDF einzuhalten.

3.3 Dokumentation

Der GB-IST ist verpflichtet die vorhandenen RAS-Lösungen samt der darüber vergebenen Berechtigungen zentral zu dokumentieren, um somit gemäß der Richtlinie für das Administratorenwesen im ZDF jederzeit auskunftsfähig zu sein.

Die festgelegten Vorgaben (RAS-Benutzer, benötigte Dienste, Verschlüsselungs- und Authentifizierungsverfahren, Zugangs- und Zugriffsberechtigungen usw.) sowie die technische Realisierung sind in einer Betriebsdokumentation zu beschreiben.

3.4 Verhalten bei Störungen und Sicherheitsvorfällen

Jeder RAS-Anwender muss Störungen und Unregelmäßigkeiten umgehend dem zuständigen Fachbereich des GB-IST melden, der wiederum seinen zuständigen IT-Sicherheitsmanager informiert. Die weitere Benutzung des betroffenen RAS-Zugangs durch den Benutzer hat in diesen Fällen sofort zu unterbleiben. Notfalls, bei Gefahr in Verzug, dürfen Seitens des GB-IST bestehende RAS-Verbindungen unmittelbar beendet oder RAS-Zugänge deaktiviert werden.

Bei einem Sicherheitsvorfall sind alle relevanten Informationen (z.B. Logfiles, Endgerät, ...) zur weiteren Untersuchung zu sichern.

3.5 Schulungen/Unterweisungen

Um einen sicheren Umgang und sachgemäße Nutzung von RAS-Zugängen gewährleisten zu können, sind entsprechende Einweisungen und Schulungen für RAS-Anwender durchzuführen. Entsprechende Anwender- und Sicherheitshinweise sind durch den GB-IST zu erstellen und für alle RAS-Anwender zugänglich zu machen (z.B. Merkblatt). Der RAS-Anwender muss darüber hinaus über den Umfang der stattfindenden Protokollierung und Auswertung (siehe Abschnitt 4.5) informiert werden. Auch die Abläufe zur Entstörung oder bei Sicherheitsvorfällen müssen dem Anwender mitgeteilt werden.

Die Anwender sind dazu verpflichtet diesen Hinweisen Folge zu leisten. Generell gelten für RAS-Anwender die gleichen Vorgaben zur IT-Sicherheit, wie für die Anwender im lokalen Netz des ZDF.



4 Sicherheitstechnische Anforderungen

4.1 IT-Endgeräte

Die für den Remote Access vorgesehenen Endgeräte müssen den spezifischen Sicherheitsanforderungen des entsprechenden RAS-Typ und Anwendungszwecks gerecht werden. Ausschlaggebend ist hier zum einen der Schutzbedarf der vom Remote Access betroffenen Ressourcen, Dienste oder Anwendungen. Zum anderen muss die zum Einsatz kommende RAS-Variante und damit einhergehenden spezifischen Gefährdungen in Betracht gezogen werden. Hier gilt es bereits während der Planung eines Remote Access Verfahrens entsprechende Festlegungen für zugelassene IT-Endgeräte zu treffen.

4.2 Verschlüsselung

Grundsätzlich ist bei jeder RAS-Verbindung die Vertraulichkeit und Integrität der Daten während des Transports sicher zu stellen. Besitzt der Transportweg einen nicht mit dem Bürokommunikationsnetzwerk vergleichbaren Vertrauensstatus, dann ist eine angemessene Verschlüsselung des Transportwegs zu etablieren.

Dabei ist folgendes zu beachten:

- Der Schlüsselaustausch muss mit einem sicheren Verfahren bei ausreichender Schlüssellänge durchgeführt werden.
- Die Speicherung des Authentisierungsschlüssels darf auf den beteiligten Systemen nicht unverschlüsselt sein.
- Für den Schutz der Authentisierungsschlüssel müssen sichere Passwörter gewählt werden.
- Die technische Richtlinie BSI TR-02102 in der jeweils aktuellen Version ist zu beachten.

Bei RAS-Verbindungen auf der Presentation-Ebene ist ebenfalls zwischen Endgerät und Presentation-Server eine angemessene Verschlüsselung zu etablieren.

4.3 Authentifizierung

Zur Authentifizierung am RAS-/Sicherheitgateway sind angemessen starke Authentifizierungsmechanismen (z.B. 2-Faktor-Authentifizierung mit Besitz und Wissen) zu verwenden.

4.4 Zugangs- und Zugriffskontrolle

RAS-Benutzer müssen sich über das RAS-Gateway eindeutig identifizieren. Ihre Identität muss bei jedem neuen Verbindungsaufbau sichergestellt werden. Der RAS-Zugang ist auf das zur Aufgabenerfüllung notwendige Maß (Least Privilege) zu begrenzen. Die Berechtigungen sind an den jeweiligen Stellen entsprechend zu setzen.

4.5 Protokollierung

Die Nutzung über einen RAS-Zugang muss nachvollziehbar sein. Dazu sind die Verbindungsdaten zu protokollieren und 30 Tage sicher aufzubewahren. Der GB-IST stellt dabei eine zeitnahe Auswertung der Protokolldaten auf Unregelmäßigkeiten sicher, um einen



Missbrauch rechtzeitig erkennen zu können. Die dazu zur Anwendung kommenden Mechanismen sind transparent zu machen.

Im Falle eines vermuteten Missbrauchs sind umgehend die Maßnahmen zur Sicherheitsvorfallbehandlung einzuleiten (siehe Abschnitt 3.4).