Bundesnetzagentur

Informationssicherheitsmanagement der Bundesnetzagentur

Fernwartungsrichtlinie (Auszug bei Ausschreibungen)

06.01.2022

Dokumentinformationen

Sperrvermerk	Offen in der BNetzA und beim Vergabeverfahren (etc.)
Dateiname	Anlage 08 - Auszug FernwartungsRL.docx
Letzte Bearbeitung (Speicherdatum)	04.08.2026 08:45:00
Aktuelles Datum	04.08.2026
Seitenzahl	9

Dokument-Status und –Freigabe		
	Datum	Name
Erstellt	12.02.2016	IS17-SIB2
Revision	12.02.2016	IS17-SIB; IS13-10
Freigabe	19.04.2022	Bernhard Grote-Bautz, ISB

Änderungsnachweis				
Versions-Nr.	Status	Bearbeiter	Datum	Änderung / Bemerkung
0.1	draft	IS17-SIB2	12.02.2016	Initiale Version
0.2	reviewed	IS17-SIB	12.02.2016	Zwischenstand
0.3	reviewed	IS13-10	15.02.2016	Ergänzungen (Checkliste) und Streichungen (VPN Hinweise)
0.4	reviewed	IS17-SIB	18.03.2019	Aktualisierung (Neuer GS)
0.41	reviewed	IS-SIB	19.04.2022	Anpassung Layout

Inhaltsverzeichnis

1. Geltungsbereich

Das vorliegende Dokument ist ein Auszug aus der aktuellen Fernwartungsrichtlinie der BNetzA. Es dient der Ergänzung von Ausschreibungs-, Vergabe- und Vertragsunterlagen. Als Anlage zum Dokument „Besondere Bestimmungen zur Informationssicherheit“ kann es die dort getroffenen Regelungen nicht einschränken.

2. Grundprinzipien

1. Berücksichtigung der für die verwendeten technischen Systeme, Übertragungseinrichtungen und organisatorischen Aspekte jeweils gültigen relevanten Grundschutz-Bausteine bzw. Grundschutz-Maßnahmen.

2. Zur Durchführung der Fernzugriffe über Fernzugänge dürfen ausschließlich Systeme und Übertragungseinrichtungen verwendet werden, deren sicherheitsrelevante Eigenschaften und Einsatzumgebungen der technischen und organisatorischen Kontrolle der BNetzA unterliegen.

3. Die Durchführung der Fern-Zugriffe sowie der Zugang zu den, den Fernzugängen unterliegenden Komponenten und Verfahren ist nur für vertrauenswürdige Dienstleister (gemäß definierter Qualitätskriterien wie z.B. einschlägiger Referenzen, Reputationen, qualifiziertem und evtl. überprüftem Personal, Einhaltung von Standards) sowie für von der BNetzA persönlich ermächtigte Mitarbeiter möglich.

4. Die Fernzugriffe setzen eine erfolgreiche und gegenseitige Authentifizierung von Mitarbeitern, Endgeräten und Komponenten sowie Netzen und Sicherheitszonen voraus.

5. Die Kommunikation zwischen dem Vertrauensbereich der BNetzA und den für die Fernzugriffe verwendeten Endgeräten unterliegt einer grundsätzlichen Verschlüsselung.

6. Auf den verwendeten Endgeräten findet grundsätzlich keine dauerhafte Speicherung von Administrations-, Konfigurations- oder Nutzdaten der BNetzA statt. Ist eine temporäre Speicherung über die Dauer einer Session hinaus erforderlich, so sind diese Daten mit einem, dem Schutzbedarf angemessenen Verfahren zu verschlüsseln.

7. Fernzugang und -zugriff erfolgen grundsätzlich nur innerhalb von Bereichen des Informationsverbundes, die eine ausreichende Separation der Netze, Komponenten, Anwendungen und Verfahren unter Berücksichtigung der Schutzbedarfsanforderungen gewährleisten.

8. Alle Aktivitäten im Rahmen der Gewährung, Nutzung und Deaktivierung von Zugängen sowie alle Zugriffe unterliegen einer Protokollierung und Steuerung sowie einem Monitoring durch die BNetzA.

3. Organisatorische Maßnahmen

Die nachfolgenden Abschnitte beschreiben organisatorische Anforderungen sowie Anforderungen an Prozesse im Rahmen der Einrichtung, Durchführung, Anpassung, Überprüfung und Beendigung von Fernzugängen und Tätigkeiten im Rahmen von Fernzugriffen.

Jeder (externe) Mitarbeiter, der Fernzugriffe durchführen soll, muss von der BNetzA individuell hierzu ermächtigt werden. Dazu ist ein Registrierungs- und Ermächtigungsprozess gemäß der nachfolgenden Rahmenbedingungen durchzuführen:

- Individuelle und namentliche Identifizierung von Mitarbeitern.
- Verpflichtung von Mitarbeitern auf Einhaltung der Bedingungen an die Endgeräte sowie deren Einsatz.
- Einverständniserklärung von Mitarbeitern sowie von Dienstleistern zur Protokollierung und Auswertung relevanter Protokolldaten im Rahmen der Überwachung und Steuerung der Fernzugriffe sowie zur Behandlung von Sicherheitsvorfällen.
- Vertragliche Verpflichtung von Dienstleistern auf die Einhaltung der Regelungen für Dienstleister [in Punkt drei].
- Zuteilung von geeigneten Fernzugangsrollen sowie zugehörigen (eingeschränkten) Rechten gemäß der Rechte- und Rollenkonzepte für die dem Fernzugriff unterliegenden Systeme.
- Zuteilung von individuellen, zeitlich begrenzten Kennungen.
- Ausgabe und Freischaltung von individuellen Zugangsdaten oder –token mit einem ausreichend sicheren Verfahren.

4. Dienstleister

Als Dienstleister im Sinne der vorliegenden Richtlinie sind externe Unternehmen oder Organisationen zu verstehen, die im Auftrag der BNetzA Fernzugriffe für Fernwartung oder Fernadministration unter Nutzung von Fernzugängen durchführen. Neben der im vorhergehenden Abschnitt beschriebenen Anforderungen an die Ermächtigung der Mitarbeiter eines Dienstleisters muss die Auswahl und Beauftragung der Dienstleister durch die BNetzA grundsätzlich folgenden Anforderungen genügen:

- Es müssen Dienstleister ausgewählt werden, die über eine nachgewiesene Zuverlässigkeit verfügen und auch die Zuverlässigkeit der Mitarbeiter sicherstellen und nachweisen können. Geeignete Nachweise sind auf Aufforderung vorzulegen.
- Die Beauftragung zur Durchführung der Fernzugriffe muss immer auf einer vertraglichen Grundlage geschehen, die die Zuverlässigkeit des Dienstleisters sowie den Einsatz zuverlässiger Mitarbeiter und deren Verpflichtung auf die o.a. Richtlinien bzw. deren sinngemäße Umsetzung festschreibt.

- Der Dienstleister muss auf die Einhaltung der in den o.a. Richtlinien formulierten Sicherheitsanforderungen an die in seinem Verantwortungsbereich liegenden IT-Komponenten (Endgeräte, Kommunikationssysteme, Kommunikationsverbindungen) sowie an deren Einsatzumgebungen verpflichtet werden.

Insbesondere sind in jedem Fall auf Seiten des Dienstleisters verantwortliche Mitarbeiter des Informationssicherheitsmanagements zu benennen, die eine Abstimmung der Sicherheitsmaßnahmen sowie eine zuverlässige Behandlung von Sicherheitsvorfällen in Zusammenarbeit mit dem Informationssicherheitsmanagement der BNetzA sicher stellen können.

4.1 Weiterführende Dokumentation

Die nachfolgenden Grundschutz-Maßnahmen bieten weiterführende Informationen und Anforderungen im Umfeld der Fernzugriffe sowie von Fernzugängen im Allgemeinen. Die Auflistung dient der weiterführenden Information und erhebt keinen Anspruch auf Vollständigkeit. Eine vollständige Übersicht der direkt und indirekt relevanten Grundschutzmaßnahmen findet sich in den jeweils aktuellen Ausgaben der Grundschutz-Kompendium des BSI.

- OPS.2.4 Fernwartung
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_2_4_Fernwartung.html

Zusätzliche detaillierte und weiterführende Informationen zu den Anforderungen für Fernzugriffe sowie Ausprägungen von möglichen technischen und organisatorischen Maßnahmen finden sich auch in der Studienreihe ISi-Fern des BSI. Diese kann auf den Internetseiten des BSI unter https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Fern/isi-fern.html heruntergeladen werden.

4.2 Anforderungsliste zur Fernadministration für Dienstleister

In der folgenden Tabelle sind die Anforderungen zur Durchführung der Fernadministration und –wartung für einen Dienstleister der Bundesnetzagentur zusammengestellt.

Anforderungen an Endgeräte
Einsatz unter sicheren Einsatz- und Umgebungsbedingungen
Keine dauerhafte Datenspeicherung und sichere Löschung bei temporärer Speicherung
Beschränkung des Zugangs zum Endgerät auf autorisierte Mitarbeiter
Maßgaben zur Verwendung externer Datenträger (Terminal-Session, muss ausgeschaltet werden)
Aufbau einer ausreichend verfügbaren und performanten Kommunikationsverbindung
Anforderungen an Mitarbeiter
Persönliche Ermächtigung der Mitarbeiter für den Fernzugriff
Verpflichtung auf den sorgfältigen und sicherheitsbewussten Umgang mit Zugangsdaten und Token
Verpflichtung auf den sorgfältigen und sicherheitsbewussten Umgang mit dem Endgerät
Verpflichtung auf die Einhaltung von Maßnahmen zur Vermeidung eines Verlusts oder Diebstahls
Verpflichtung zur sicheren und getrennten Aufbewahrung des Endgerätes und Tokens bei deren Nichtnutzung
Verpflichtung zur Nutzung der Endgeräte nur unter Umgebungsbedingungen, die einen Schutz vor Kompromittierung und missbräuchliche Verwendung durch unbefugte Dritte gewährleisten
Verpflichtung auf die sorgfältige und sicherheitsbewusste Initiierung, Durchführung und Beendigung der administrativen Tätigkeiten
Verpflichtung auf den sorgfältigen und sicherheitsbewussten Umgang mit Daten der BNetzA, die im Zusammenhang mit der Fernadministration oder -wartung erfasst, gespeichert oder übertragen werden
Verpflichtung auf die regelmäßige und verschlüsselte Sicherung von Daten, die nur auf dem Endgerät vorliegen und für die Fernadministration oder -wartung erforderlich sind
Verpflichtung auf den Ausschluss der privaten Nutzung des Endgerätes bzw. dessen technischer Ausstattung und Zubehörs
Einverständnis zur Protokollierung, Steuerung und zum Monitoring der Tätigkeiten im Rahmen der Fernadministration und -wartung
Einweisung für das Verhalten bei Verlust oder Verdacht der Kompromittierung des Endgerätes, dessen Zubehör, der Authentisierung und Identifizierung sowie der Kommunikationsverbindung
Verpflichtung, keine Nutz- oder Konfigurationsdaten aus dem Netz der BNetzA heraus zu exportieren
Verpflichtung zur Beschränkung der Aktivitäten auf das fachlich Notwendige

Nachweis über Sicherheitsüberprüfung (Sabotageschutzerklärung) und Belehrung der Mitarbeiter
Verpflichtung auf die Einhaltung der Sicherheitsanforderungen an die in seinem Verantwortungsbereich liegenden IT-Komponenten (Endgeräte, Kommunikationssysteme, Kommunikationsverbindungen) sowie an deren Einsatzumgebungen
Individuelle und namentliche Identifizierung der Mitarbeiter, die Fernadministrationen und -wartungen durchführen
Anforderungen an Verbindungen
Auswahl eines geeigneten Netzzugang sowie eines geeigneten Transfernetzes
Ausreichende Bandbreite und Verfügbarkeit der an der Kommunikationsverbindung beteiligten Komponenten (Netzzugang, Transfernetz)
Freigabe der Fernsitzung durch die BNetzA
Autorisierung zeitlich begrenzter Fernsitzungen durch BNetzA-Mitarbeiter oder BNetzA-Mechanismen unter Festlegung und Beschränkung der zulässigen Zugänge zu Komponenten und Verfahren
Automatisierte Terminierung von Sitzungen nach Ablauf des zugelassenen Zeitraumes sowie bei einem Timeout
BNetzA behält sich die Möglichkeit zur manuellen oder automatisierten Zwangstrennung vor
Sitzungsbezogene Zuweisung der Verbindung zu einem Zielsystem-Proxy innerhalb der Fernwartungszone
Überprüfung auf Schadsoftware oder Angriffsmuster innerhalb der Fernwartungszone
Terminierung verschlüsselter Protokolle innerhalb der Fernwartungszone
Überwachung und Steuerung von Fernzugriffsaktivitäten durch BNetzA-Mitarbeiter
Protokollierung der Verbindungen und Aktivitäten innerhalb der Fernzugriffszone
Separation der Verbindungen innerhalb der Fernzugriffszone unter Berücksichtigung der Anforderungen an den Schutzbedarf sowie im Hinblick auf eine Mandantentrennung
Beschränkung der Zugänge auf die für die Sitzung erforderlichen Zielsystemen im LAN
Zuordnung von Fernzugriffsrollen mit eingeschränkten Rechten für den Zugriff
Beschränkung der Zugriffsrechte auf das erforderliche Maß
(Revisions-) Sichere Protokollierung der individuellen Tätigkeiten der Sitzung mit eindeutiger Zuordnung zu Nutzerkennungen
Ausschluss von Verbindungen zwischen dem Zielsystem und externen unsicheren Netzen (insbesondere Internet)

5. Abkürzungsverzeichnis

AG	Auftraggeber
AN	Auftragnehmer
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
ISB / IT-SiBe	Informationssicherheitsbeauftragter / IT-Sicherheitsbeauftragter
ISM	Informationssicherheitsmanagement
ISMS	Informationssicherheitsmanagementsystem
LAN	Local Area Network (lokales Netzwerk)
RL	Richtlinie
Token	Hilfsmittel zur Identifizierung und Authentifizierung
UP BUND 2017	Umsetzungsplan Bund 2017