|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Fernwartung"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300018 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Fernwartung" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc79433328)

[Dokumentenhistorie 3](#_Toc79433329)

[Inhaltsverzeichnis 4](#_Toc79433330)

[Allgemeine Festlegungen 5](#_Toc79433331)

[Ziel / Zweck 5](#_Toc79433332)

[Geltungsbereich 5](#_Toc79433333)

[Zuständigkeiten 6](#_Toc79433334)

[Genehmigungs- und Änderungsverfahren 6](#_Toc79433335)

[Aufbau des Dokuments 6](#_Toc79433336)

[Sicherheitsrichtlinie „Fernwartung" 7](#_Toc79433337)

[Basismaßnahmen 7](#_Toc79433338)

[Planung des Einsatzes der Fernwartung (OPS.1.2.5.A1) 7](#_Toc79433339)

[Sicherer Verbindungsaufbau bei der Fernwartung (OPS.1.2.5.A2) 7](#_Toc79433340)

[Absicherung der Kommunikationsverbindungen bei der Fernwartung (OPS.1.2.5.A3) 7](#_Toc79433341)

[Regelungen zu Kommunikationsverbindungen (OPS.1.2.5.A4) 7](#_Toc79433342)

[Standardmaßnahmen 7](#_Toc79433343)

[Einsatz von Online-Diensten (OPS.1.2.5.A5) 8](#_Toc79433344)

[Dokumentation bei der Fernwartung (OPS.1.2.5.A7) 8](#_Toc79433345)

[Sichere Protokolle bei der Fernwartung (OPS.1.2.5.A8) 8](#_Toc79433346)

[Auswahl geeigneter Fernwartungswerkzeuge (OPS.1.2.5.A9) 8](#_Toc79433347)

[Verwaltung der Fernwartungswerkzeuge (OPS.1.2.5.A10) 8](#_Toc79433348)

[Einsatz von kryptografischen Verfahren bei der Fernwartung (OPS.1.2.5.bd.A1) 8](#_Toc79433349)

[Patch- und Änderungsmanagement bei der Fernwartung (OPS.1.2.5.bd.A2) 8](#_Toc79433350)

[Datensicherung bei der Fernwartung (OPS.1.2.5.bd.A3) 9](#_Toc79433351)

[Absicherung der Fernwartung (OPS.1.2.5.bd.A4) 9](#_Toc79433352)

[Schulungen zur Fernwartung (OPS.1.2.5.bd.A5) 9](#_Toc79433353)

[Authentisierungsmechanismen bei der Fernwartung (OPS.1.2.5.A17) 9](#_Toc79433354)

[Passwortsicherheit bei der Fernwartung (OPS.1.2.5.bd.A6) 9](#_Toc79433355)

[Fernwartung durch Dritte (OPS.1.2.5.A19) 10](#_Toc79433356)

[Betrieb der Fernwartung (OPS.2.4.A20) 10](#_Toc79433357)

[Erstellen eines Notfallplans für den Ausfall der Fernwartung (OPS.1.2.5.A21) 10](#_Toc79433358)

[Absicherung integrierter Fernwartungssysteme (OPS.1.2.5.A24) 10](#_Toc79433359)

[Maßnahmen bei erhöhtem Schutzbedarf 10](#_Toc79433360)

[Dedizierte Systeme bei der Fernwartung (OPS.1.2.5.A14 - CIA) 11](#_Toc79433361)

[Redundante Verwendung von mobilen Kommunikationsnetzen (OPS.1.2.5.A22 - A) 11](#_Toc79433362)

# Allgemeine Festlegungen

## Ziel / Zweck

Mit dem Begriff Fernwartung wird bei der <Institution> ein räumlich getrennter Zugriff auf IT-Systeme und die darauf laufenden Anwendungen bezeichnet. Der Zugriff kann z. B. dazu dienen, Konfigurations-, Wartungs- oder Reparaturarbeiten durchzuführen.

Die Fernwartung kann aktiv oder passiv geschehen. Bei der aktiven Fernwartung werden die Tastatur- und Maussignale vom System eines Administrators an ein entferntes System übertragen. Das entfernte System überträgt die Bildschirm- oder Konsolenausgabe an das System des Administrators. Der Administrator führt Aktionen auf dem entfernten System aus, als wenn er selbst vor Ort wäre.

Bei der passiven Fernwartung werden nur die Bildschirminhalte (bspw. durch die Nutzung von Microsoft Teams, Hangout, WebEx oder anderen WebRTC-Diensten) eines Systems zum Administrator übertragen. Der Administrator erteilt einem Mitarbeitenden vor Ort Anweisungen, die vom Mitarbeitenden ausgeführt und vom Administrator beobachtet werden.

Da sich viele IT-Systeme außerhalb der Reichweite der verantwortlichen Administratoren befinden (z. B. in entfernten Rechenzentren oder einem Außenstandort ohne IT-Personal), setzt die <Institution> die Möglichkeiten der Fernwartung ein. Aufgrund der tiefgreifenden Eingriffsmöglichkeiten in IT-Systeme, ist die Absicherung von Fernwartungskomponenten von besonderer Bedeutung.

Ziel dieser Sicherheitsrichtlinie ist der Schutz der Informationen, die auf Basis der Fernwartung gespeichert, verarbeitet und übertragen werden sowie der Schutz der Fernwartungsschnittstellen von IT-Systemen. Zu diesem Zweck werden Anforderungen an die Fernwartung gestellt, die sich auf Funktionen der aktiven und passiven Fernwartung beziehen. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Baustein OPS.1.2.5 "Fernwartung" zurückgegriffen.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Das Dokument „Sicherheitsrichtlinie Fernwartung“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Fernwartung"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Planung des Einsatzes der Fernwartung (OPS.1.2.5.A1)

Der Einsatz der Fernwartung muss an die <Institution> angepasst und bedarfsgerecht hinsichtlich technischer und organisatorischer Aspekte geplant werden. Es ist zu klären, ob In-Band und/oder Out-Band Administration genutzt wird, welche IT-Systemschnittstellen und Protokolle verwendet werden. Es ist ebenfalls zu klären, wie die Fernwartung abgesichert wird und wie die genutzten Lösungen auditiert werden. Im Rahmen der Planung der Fernwartung sind auch die Anforderungen aus dem Notfallmanagement mit zu berücksichtigen.

### Sicherer Verbindungsaufbau bei der Fernwartung (OPS.1.2.5.A2)

Die Initiierung des Zugriffs für die Fernwartung muss aus der <Institution> heraus erfolgen. Der Benutzer des fernadministrierten IT-Systems muss dem Fernzugriff explizit zustimmen.

### Absicherung der Kommunikationsverbindungen bei der Fernwartung (OPS.1.2.5.A3)

Die freigegeben Zugänge und Kommunikationsschnittstellen für einen Verbindungsaufbau von Außen sind auf das notwendige Maß zu beschränken. Ebenso sind alle Kommunikationsverbindungen nach vollzogenem Fernzugriff zu deaktivieren. Für die Fernwartung sind die freigegebenen und notwendigen Ports über entsprechende Firewall-Regeln ständig bereitzustellen. Es sind unter Berücksichtigung des erforderlichen Schutzbedarfes des IT-Systems oder der Anwendung sichere Authentisierungsmechanismen (z. B. SSO mit 2FA) für die Administratoren einzusetzen.

### Regelungen zu Kommunikationsverbindungen (OPS.1.2.5.A4)

Unter Beachtung der Anforderungen an den Betrieb von Firewalls müssen für die zu etablierende die Fernwartung ein Firewall-Regelwerk auf Basis von White-Lists eingebunden werden. Hierbei muss sichergestellt werden, dass bestehende Firewall-Infrastrukturen und deren Regelungen nicht umgangen werden. Die administrativen Webschnittstellen von Sprungsystemen, Absicherungssystemen oder Authentisierungssystemen dürfen nicht aus dem öffentlichen Netz direkt erreichbar sein.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Einsatz von Online-Diensten (OPS.1.2.5.A5)

Es muss im Rahmen der Planung der Fernwartung entschieden werden, ob eine Fernwartung über Online-Dienste (Cloud-Services) erlaubt ist und welche Art von Cloud-Services genutzt werden dürfen. Es sollten technische und organisatorische Maßnahmen ergriffen werden, um sicher zu stellen, dass nur die freigegeben Services genutzt werden können. Die Clients für die Fernwartung sollten automatisiert keine Verbindungen zum Online-Dienst aufbauen.

### Dokumentation bei der Fernwartung (OPS.1.2.5.A7)

Alle genutzten Möglichkeiten zur Fernwartung sind für einen sicheren Betrieb zu dokumentieren. In diesem Dokument ist der Aufbau des Fernwartungssystems sowie die Arbeitsweise und der zur Initiierung einer Fernwartung berechtigten Personen aufzuzeigen. Nur die relevanten Personen dürfen auf diese Informationen zu greifen.

### Sichere Protokolle bei der Fernwartung (OPS.1.2.5.A8)

Die Fernwartung erfolgt nur über die von der <Institution> freigegebene, kryptographische Kommunikationsprotokolle und deren Algorithmen und Schlüssellängen.

### Auswahl geeigneter Fernwartungswerkzeuge (OPS.1.2.5.A9)

Die Beschaffung erfolgt aufgrund von betrieblichen, sicherheitstechnischen und datenschutzrechtlichen Anforderungen, die mit allen relevanten Departments der <Institution> abgestimmt sind.

### Verwaltung der Fernwartungswerkzeuge (OPS.1.2.5.A10)

Die zur Initiierung einer Fernwartung berechtigten Personen sind auf den Systemen geschult und bei auftretenden Problemen können sie sich an einen, für das System verantwortlichen, Ansprechpartner wenden.

Es sind organisatorische Prozesse zum Umgang mit den vom der <Institution> zur Verfügung gestellten Werkzeugen zu etablieren. Es sollte eine Bedienungsanleitung beziehungsweise ein Handzettel für den Umgang mit dem Fernwartungswerkzeug vorliegen.

### Einsatz von kryptografischen Verfahren bei der Fernwartung (OPS.1.2.5.bd.A1)

Um die Kommunikation abzusichern und die Administrierenden zu authentisieren, dürfen bei der Fernwartung nur von der <Institution> freigegebene ausreichend starke kryptografische Verfahren genutzt werden. Die Stärke der verwendeten kryptografischen Verfahren und Schlüssel sollten im Rahmen der Fernwartung regelmäßig überprüft und, falls erforderlich, angepasst werden.

### Patch- und Änderungsmanagement bei der Fernwartung (OPS.1.2.5.bd.A2)

Es sind die allgemeinen Vorgaben zum Patch- und Änderungsmanagement der <Institution> für die Fernwartung umzusetzen. Die IT-Systeme und Administrationswerkzeuge sollten alle im Patch- und Änderungsmanagement berücksichtigt werden.

Die Fernwartungszugänge sind geeignet zu aktivieren und zu deaktivieren. Alle Aktivierungen und Deaktivierungen der Fernwartungszugänge für Third Parties sind zusätzlich zu dokumentiert. Aus Sicherheitsgründen sind alle für die Fernwartung benötigten IT-Systeme und Anwendungen zeitnah zu aktualisieren. Bevor Patches und Änderungen eingespielt werden, sollten diese vorab in einer geeigneten Testumgebung geprüft werden.

### Datensicherung bei der Fernwartung (OPS.1.2.5.bd.A3)

Zur Vermeidung von Datenverlusten innerhalb der Infrastruktur für die Fernwartung sollten regelmäßige Datensicherungen erfolgen. Es sollten Vorgaben der Datensicherung bei der Fernwartung anhand der Menge und Wichtigkeit der laufend neu gespeicherten Daten und des möglichen Schadens für die <Institution> bei Verlust dieser Daten getroffen werden.

Alle Datensicherungsanforderungen der Fernwartung sind mit den allgemeinen Vorgaben der <Institution> zur Datensicherung korrespondieren.

### Absicherung der Fernwartung (OPS.1.2.5.bd.A4)

Die Fernwartung sollte nur aus dem internen Netz der <Institution> erfolgen.

Falls es dennoch nötig ist, von einem öffentlichen Datennetz auf interne IT-Systeme zuzugreifen, dürfen nur abgesicherte Virtuelles Privates Netz (VPN) genutzt werden. Für die Fernwartung per VPN ist eine kryptographisch abgesicherte Verbindung zu etablieren. Neben diesen externen Fernwartungszugängen sind auch die internen Fernwartungszugänge abzusichern. Die Benutzung von internen Fernwartungszugängen ist auf der Basis des need-to-know Prinzips einzuschränken. Des Weiteren sollten alle Aktivitäten während einer Administrationssitzung protokolliert werden.

### Schulungen zur Fernwartung (OPS.1.2.5.bd.A5)

Alle zur Initiierung einer Fernwartung berechtigen Personen sind im Umgang mit den bereitgestellten Werkzeugen zu schulen. Notwendige Eskalationsmechanismen sind den berechtigen Personen ebenfalls zu benennen.

### Authentisierungsmechanismen bei der Fernwartung (OPS.1.2.5.A17)

Für die Fernwartung sind SSO und 2FA-Verfahren zur Authentisierung einzusetzen. Zur Erleichterung der Anmeldung bei der Fernwartung ist diese in einem Identitäts- und Berechtigungsmanagement und deren Infrastrukturen zu integrieren.

### Passwortsicherheit bei der Fernwartung (OPS.1.2.5.bd.A6)

Falls bei der Fernwartung passwortbasierte Authentisierungen verwendet wird, sind die Passwortregeln der <Institution> einzuhalten. Für die Fernwartung sind die Passwortregeln der <Institution> technisch zu forcieren.

### Fernwartung durch Dritte (OPS.1.2.5.A19)

Wenn es nicht möglich ist, auf externe Fernwartung seitens der <Institution> zu verzichten, sollten alle Aktivitäten des Dienstleisters von Internen Mitarbeiter beobachtet werden. Alle Fernwartungsvorgänge durch den Dienstleister sollten aufgezeichnet werden. Mit externem Wartungspersonal sind vertragliche Regelungen zu treffen, welche sicherstellen, dass diese die Vorgaben der <Institution> einhalten und entsprechende fachliche Kompetenzen aufweisen.

### Betrieb der Fernwartung (OPS.2.4.A20)

Es ist mittels eines Ticketsystems ein Meldeprozess für Support- und Fernwartungsanliegen zu etablieren. Alle Zugriffe durch die Fernwartung dürfen erst nach erfolgreicher Authentisierung (SSO und 2FA-Verfahren) gestattet werden.

Die zur Etablierung der Fernwartungszugänge erforderlichen Freischaltungen an der Sicherheitsinfrastruktur sind in die etablierten Prozesse für Firewall-Regeln seitens der <Institution> zu integrieren. Es sind Mechanismen zur Erkennung und Abwehr von hochvolumigen Angriffen, TCP-State-Exhaustion- Angriffen und Angriffen auf Applikationsebene zu implementieren.

Alle Fernwartungsvorgänge sollten aufgezeichnet werden. Die anfallenden Protokolldaten sind regelmäßig auszuwerten.

### Erstellen eines Notfallplans für den Ausfall der Fernwartung (OPS.1.2.5.A21)

Sind die Verfügbarkeitsanforderungen an die Fernwartung entsprechend hoch, ist das Fernwartungssystem Bestandteil des zentralen Notfallmanagements und für die Wiederherstellung ist ein Notfallplan zu erstellen und die Umsetzbarkeit regelmäßig zu prüfen.

### Absicherung integrierter Fernwartungssysteme (OPS.1.2.5.A24)

Bei der Beschaffung von neuen IT-Systemen sollte geprüft werden, ob diese Systeme oder einzelne Komponenten der Systeme über Funktionen zur Fernwartung verfügen. Werden diese Funktionen nicht verwendet, sind diese Funktionen zu deaktivieren. Die Funktionen sind ebenfalls zu deaktivieren, wenn diese Funktionen durch bekannte Sicherheitslücken gefährdet sind.

Werden Fernwartungsfunktionen verwendet, die in die Firmware einzelner Komponenten integriert sind, sollten deren Funktionen und der Zugriff darauf so weit wie möglich eingeschränkt werden. Die IT-Systeme und Anwendungen dürfen nur aus einem getrennten Management-Netz erreichbar sein.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Dedizierte Systeme bei der Fernwartung (OPS.1.2.5.A14 - CIA)

Innerhalb der Fernwartung sind Komponenten einzusetzen, die ausschließlich diesem Anwendungszweck dienen. Alle weiteren Funktionen/Dienste sind zu deaktivieren. Die Komponenten für die Fernwartung sind zu härten und somit sicher zu konfigurieren.

### Redundante Verwendung von mobilen Kommunikationsnetzen (OPS.1.2.5.A22 - A)

Sind die Verfügbarkeitsanforderungen an die Fernwartung entsprechend hoch, sollten redundante Verbindungs- bzw. Kommunikationsnetze eingerichtet werden.