Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.2.5 Fernwartung

1. Beschreibung

1.1. Einleitung

Mit dem Begriff Fernwartung wird ein zeitlich begrenzter Zugriff auf IT-Systeme und die darauf laufenden Anwendungen bezeichnet, der von einem anderen IT-System aus erfolgt. Der Zugriff kann z. B. dazu dienen, Konfigurations-, Wartungs- oder Reparaturarbeiten durchzuführen.

Die Fernwartung kann auf unterschiedliche Weise geschehen. Bei der Fernwartung von Clients werden oft die Tastatur- und Maussignale von IT-Systemen von den Administrierenden an ein entferntes IT-System übertragen. Das entfernte IT-System überträgt die Bildschirmausgabe an das IT-System der Administrierenden. Die Administrierenden führen Aktionen auf dem entfernten IT-System so aus, als wenn sie selbst vor Ort wären (aktive Fernwartung). Bei der Fernwartung von Servern wird oft die Ein- und Ausgabe der Konsole übertragen.

Bei der passiven Fernwartung werden nur die Bildschirminhalte eines IT-Systems zu den Administrierenden übertragen. Administrierende erteilen den Benutzenden vor Ort Anweisungen, die von ihnen ausgeführt und von den Administrierenden beobachtet werden. Allerdings erweist sich dieses Vorgehen in der Praxis meist als sehr zeitintensiv und umständlich, weshalb häufig dem IT-Betrieb voller Zugriff über das IT-System zugewiesen wird.

Da sich viele IT-Systeme außerhalb der Reichweite ihrer Administrierenden befinden (z. B. in entfernten Rechenzentren, Industrieanlagen oder einem Außenstandort ohne IT-Personal), wird Fernwartung in vielen Institutionen eingesetzt. Bei der Fernwartung wird oft über unsichere Netze auf interne IT-Systeme und Anwendungen einer Institution zugegriffen. Wegen der dabei bestehenden tiefgreifenden Eingriffsmöglichkeiten in diese IT-Systeme und Anwendungen ist die Absicherung von Fernwartungskomponenten von besonderer Bedeutung.

1.2. Zielsetzung

Ziel dieses Bausteins ist der Schutz der Informationen, die bei 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 gleichermaßen auf Funktionen der aktiven und passiven Fernwartung beziehen.

1.3. Abgrenzung und Modellierung

Der Baustein ist auf alle Zielobjekte im Informationsverbund anzuwenden, bei denen Fernwartung genutzt wird.

Dieser Baustein betrachtet die Fernwartung überwiegend aus der Sicht des IT-Betriebs und gibt Hinweise für Administrierende, wie Fernwartung eingesetzt werden kann. Die Sicherheitsaspekte der eingesetzten Kommunikationsverbindungen und Authentisierungsmechanismen sowie die Absicherung der Fernwartungszugänge sind wichtige Bestandteile dieses Bausteins. Dennoch werden darin nicht alle relevanten Aspekte der mit einer Fernwartung in Verbindung stehenden Geschäftsprozesse abgedeckt. Vor allem die Bausteine OPS.1.1.3 *Patch- und Änderungsmanagement*, ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*, CON.1 *Kryptokonzept* und CON.3 *Datensicherungskonzept* sind zusätzlich zu beachten. Ebenso sind die Vorgaben der Bausteinschicht NET *Netze und Kommunikation* umzusetzen, sofern diese direkt mit der Fernwartung in Verbindung stehen.

Wird die Fernwartung von externen Dienstleistenden durchgeführt, muss zudem der Baustein OPS.2.3 *Nutzung von Outsourcing* beachtet werden. Werden cloudbasierte Fernwartungsprodukte verwendet, müssen auch die allgemeinen Anforderungen aus dem Baustein OPS.2.2 *Cloud-Nutzung* erfüllt werden.

Anforderungen zur Absicherung der Fernwartung mittels Firewalls sind nicht Bestandteil dieses Bausteins. Anforderungen dazu sind im Baustein NET.3.2 *Firewall* zu finden.

Grundsätzliche Aspekte der IT-Administration werden ebenfalls nicht in diesem Baustein betrachtet. Sie sind im Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* zu finden. Ebenfalls nicht betrachtet werden Anforderungen des Systemmanagements. Diese sind im Baustein OPS.1.1.7 *Systemmanagement* zu finden.

Nicht im Fokus des Bausteins steht die Fernwartung im industriellen Umfeld. Anforderungen dazu sind im Baustein IND.3.2 *Fernwartung im industriellen Umfeld* zu finden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.2.5 *Fernwartung* von besonderer Bedeutung.

2.1. Unzureichende Kenntnisse über Regelungen der Fernwartung

Administrierende, die Fernwartung einrichten und nutzen, sind auf Regelungen angewiesen, die festlegen, wie Fernwartung verwendet werden soll. Beispielsweise ist es notwendig festzulegen, wie Anwendungen zur Fernwartung konfiguriert werden sollen. Ansonsten können mit der Fernwartung zusätzliche Risiken für das interne Netz entstehen. Werden den Beteiligten die Regelungen zur Fernwartung nicht mitgeteilt, ergeben sich Gefahren für den IT-Betrieb. Beispielsweise könnte eine Fernwartungsschnittstelle eingerichtet und dabei ein Authentisierungsverfahren mit unsicherem Passwort erlaubt werden, anstelle eines sicheren, zertifikatbasierten Verfahrens.

2.2. Fehlende oder unzureichende Planung und Regelung der Fernwartung

Wird die Fernwartung nicht sorgfältig geplant, aufgebaut und geregelt, kann die Sicherheit aller IT-Systeme einer Institution beeinträchtigt werden. Werden beispielsweise unsichere Kommunikationsprotokolle, Verschlüsselungsalgorithmen oder Authentisierungsmechanismen eingesetzt, können Sicherheitslücken entstehen. Über unzureichend gesicherte Fernwartungsschnittstellen kann auch ein gekoppeltes Netz eines Dritten kompromittiert werden.

2.3. Ungeeignete Nutzung von Authentisierung bei der Fernwartung

Bei der Fernwartung können unterschiedliche Authentisierungsmechanismen verwendet werden. Wird ein unsicheres Authentisierungsverfahren genutzt, können unberechtigte Dritte administrative Berechtigungen auf Fernwartungssystemen oder für Fernwartungswerkzeuge erlangen. Dadurch können sie auf die IT-Systeme einer Institution zugreifen und weitreichende Schäden verursachen.

Ein Beispiel hierfür ist ein Anmeldeverfahren, das nur ein kurzes Passwort verwendet. Bei einem Angriff kann dieses Passwort in kurzer Zeit erraten und sich so Zugriff auf IT-Systeme der Institution verschafft werden.

2.4. Fehlerhafte Fernwartung

Damit die Sicherheit und Funktionsfähigkeit von IT-Systemen und Anwendungen, auf die nur aus der Ferne zugegriffen werden kann, gewährleistet wird, ist eine professionelle und regelmäßige Fernwartung erforderlich. Werden solche IT-Systeme und Anwendungen nicht ordnungsgemäß per Fernwartung konfiguriert und gewartet, können sie im schlimmsten Fall nicht mehr genutzt werden. Laufen die Fernwartungsprozesse nicht korrekt ab, kann dies zu Fehlfunktionen einzelner Betriebssystemkomponenten führen. Außerdem können durch verspätete oder fehlerhafte IT-Systemwartungen Sicherheitslücken entstehen.

2.5. Verwendung unsicherer Protokolle in der Fernwartung

Die Kommunikation über öffentliche und interne Netze mittels unsicherer Protokolle stellt eine potenzielle Gefahr dar. Werden z. B. veraltete Versionen von IPSec, SSH oder SSL/TLS eingesetzt, um einen Tunnel zwischen zwei Netzen oder Endpunkten herzustellen, kann nicht gewährleistet werden, dass dieser Tunnel ausreichend sicher ist und die darin übertragenen Informationen angemessen geschützt sind. Bei einem Angriff können Schwachstellen dieser Protokolle ausgenutzt werden, um in geschützte Verbindungen eigene Inhalte einzuschleusen. Generell als unsicher gelten Protokolle, bei denen Informationen im Klartext übertragen werden.

2.6. Fehlende Regelungen zur Fremdnutzung der Fernwartungszugänge

Werden IT-Systeme von Dritten ferngewartet, ohne dass es dafür eine vertragliche Grundlage gibt, sind die Zuständigkeiten für die Fernwartung möglicherweise nicht klar geregelt. Dadurch können z. B. Rollentrennungen umgangen werden oder offene Fernwartungszugänge werden nicht dokumentiert.

2.7. Nutzung von Online-Diensten für die Fernwartung

Neben einer Fernwartung, bei der eine direkte Datenverbindung zu der betreffenden Institution aufgebaut wird, können auch Online-Dienste genutzt werden. Hierbei verbinden sich die zu administrierenden IT-Systeme mit den Servern von Online-Diensten und die Administrierenden können z. B. über einen Webbrowser auf die zu administrierenden IT-Systeme zugreifen.

Falls die Kommunikation nicht Ende-zu-Ende verschlüsselt wird, könnten die Online-Dienste den Datenaustausch mitlesen. Zusätzlich könnten auch die IT-Systeme durch unberechtigte Personen administriert werden, indem die Datenverbindung verändert wird. Bauen die IT-Systeme automatisch beim Systemstart eine Datenverbindung zum Online-Dienst auf, könnte direkt auf das IT-System zugegriffen werden, ohne dass dies den Benutzenden des IT-Systems oder den zuständigen Administrierenden bekannt ist.

2.8. Unbekannte Fernwartungskomponenten

Viele IT-Systeme enthalten Komponenten, die integrierte Funktionen zur Fernwartung bieten. Oft sind diese Funktionen aber schlecht dokumentiert und werden bei der Beschaffung sowie beim Betrieb von IT-Systemen nicht berücksichtigt.

Integrierte Fernwartungskomponenten haben weitreichenden Zugriff auf die IT-Systeme, in denen sie verbaut sind. Dieser Zugriff wirkt dabei oft direkt auf andere Komponenten des IT-Systems und kann so die Sicherheitsmechanismen des Betriebssystems umgehen. Zusätzlich können integrierte Fernwartungsfunktionen Schwachstellen enthalten, die einen unberechtigten Zugriff auf das IT-System vereinfachen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.2.5 *Fernwartung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

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

Der Einsatz der Fernwartung MUSS an die Institution angepasst werden. Die Fernwartung MUSS hinsichtlich technischer und organisatorischer Aspekte bedarfsgerecht geplant werden. Dabei MUSS mindestens berücksichtigt werden, welche IT-Systeme ferngewartet werden sollen und wer dafür zuständig ist.

OPS.1.2.5.A2 Sicherer Verbindungsaufbau bei der Fernwartung von Clients (B) [Benutzende]

Wird per Fernwartung auf Desktop-Umgebungen von Clients zugegriffen, MUSS die Fernwartungssoftware so konfiguriert sein, dass sie eine Verbindung erst nach expliziter Zustimmung der Benutzenden aufbaut.

OPS.1.2.5.A3 Absicherung der Schnittstellen zur Fernwartung (B)

Die möglichen Zugänge und Kommunikationsverbindungen für die Fernwartung MÜSSEN auf das notwendige Maß beschränkt werden. Alle Fernwartungsverbindungen MÜSSEN nach dem Fernzugriff getrennt werden.

Es MUSS sichergestellt werden, dass Fernwartungssoftware nur auf IT-Systemen installiert ist, auf denen sie benötigt wird.

Fernwartungsverbindungen über nicht vertrauenswürdige Netze MÜSSEN verschlüsselt werden. Alle anderen Fernwartungsverbindungen SOLLTEN verschlüsselt werden.

OPS.1.2.5.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

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

Die Institution SOLLTE festlegen, unter welchen Umständen Online-Dienste zur Fernwartung genutzt werden dürfen, bei denen die Verbindung über einen externen Server hergestellt wird. Der Einsatz solcher Dienste SOLLTE generell auf möglichst wenige Fälle beschränkt werden. Die IT-Systeme SOLLTEN keine automatisierten Verbindungen zum Online-Dienst aufbauen. Es SOLLTE sichergestellt werden, dass der eingesetzte Online-Dienst die übertragenen Informationen Ende-zu-Ende-verschlüsselt.

OPS.1.2.5.A6 Erstellung einer Richtlinie für die Fernwartung (S)

Die Institution SOLLTE eine Richtlinie zur Fernwartung erstellen, in der alle relevanten Regelungen zur Fernwartung dokumentiert werden. Die Richtlinie SOLLTE allen Zuständigen bekannt sein, die an der Konzeption, dem Aufbau und dem Betrieb der Fernwartung beteiligt sind.

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

Die Fernwartung SOLLTE geeignet dokumentiert werden. Aus der Dokumentation SOLLTE hervorgehen, welche Fernwartungszugänge existieren und ob diese aktiviert sind. Die Dokumente SOLLTEN an geeigneten Orten und vor unberechtigtem Zugriff geschützt abgelegt werden. Die Dokumente SOLLTEN im Rahmen des Notfallmanagements zur Verfügung stehen.

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

Nur als sicher eingestufte Kommunikationsprotokolle SOLLTEN eingesetzt werden. Dafür SOLLTEN sichere kryptografische Verfahren verwendet werden. Die Stärke der verwendeten kryptografischen Verfahren und Schlüssel SOLLTE regelmäßig überprüft und bei Bedarf angepasst werden.

Wird auf die Fernwartungszugänge von IT-Systemen im internen Netz über ein öffentliches Datennetz zugegriffen, SOLLTE ein abgesichertes Virtuelles Privates Netz (VPN) genutzt werden.

OPS.1.2.5.A9 Auswahl und Beschaffung geeigneter Fernwartungswerkzeuge (S)

Die Auswahl geeigneter Fernwartungswerkzeuge SOLLTE sich aus den betrieblichen, sicherheitstechnischen und datenschutzrechtlichen Anforderungen der Institution ergeben. Alle Beschaffungsentscheidungen SOLLTEN mit den System- und Anwendungsverantwortlichen sowie dem oder der Informationssicherheitsbeauftragten abgestimmt werden.

OPS.1.2.5.A10 Umgang mit Fernwartungswerkzeugen (S)

Es SOLLTEN organisatorische Verwaltungsprozesse zum Umgang mit den ausgewählten Fernwartungswerkzeugen etabliert werden. Es SOLLTE eine Bedienungsanleitung für den Umgang mit den Fernwartungswerkzeugen vorliegen. Ergänzend zu den allgemeinen Schulungsmaßnahmen SOLLTEN Musterabläufe für die passive und die aktive Fernwartung erstellt und kommuniziert werden. Zusätzlich zu den allgemeinen Schulungsmaßnahmen SOLLTE der IT-Betrieb besonders im Umgang mit den Fernwartungswerkzeugen sensibilisiert und geschult werden. Es SOLLTE ein Ansprechpartner oder eine Ansprechpartnerin für alle fachlichen Fragen zu den Fernwartungswerkzeugen benannt werden.

OPS.1.2.5.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.2.5.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.2.5.A13 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.2.5.A15 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.2.5.A16 ENTFALLEN (S)

Diese Anforderung ist entfallen.

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

Für die Fernwartung SOLLTEN Mehr-Faktor-Verfahren zur Authentisierung eingesetzt werden. Die Auswahl der Authentisierungsmethode und die Gründe, die zu der Auswahl geführt haben, SOLLTEN dokumentiert werden. Fernwartungszugänge SOLLTEN im Identitäts- und Berechtigungsmanagement der Institution berücksichtigt werden.

OPS.1.2.5.A18 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.2.5.A19 Fernwartung durch Dritte (S)

Wird die Fernwartung von Externen durchgeführt, SOLLTEN alle Fernwartungsaktivitäten von internen Mitarbeitenden beobachtet werden. Alle Fernwartungsvorgänge durch Dritte SOLLTEN aufgezeichnet werden.

Mit externem Wartungspersonal MÜSSEN vertragliche Regelungen über die Sicherheit der betroffenen IT-Systeme und Informationen geschlossen werden. Die Pflichten und Kompetenzen des externen Wartungspersonals SOLLTEN in den vertraglichen Regelungen festgehalten werden.

Sollten Dienstleistende mehrere Kunden und Kundinnen fernwarten, MUSS gewährleistet sein, dass die Netze der Kunden und Kundinnen nicht miteinander verbunden werden. Die Fernwartungsschnittstellen SOLLTEN so konfiguriert sein, dass es Dienstleistenden nur möglich ist, auf die IT-Systeme und Netzsegmente zuzugreifen, die für seine Arbeit benötigt werden.

OPS.1.2.5.A20 Betrieb der Fernwartung (S)

Ein Meldeprozess für Support- und Fernwartungsanliegen SOLLTE etabliert werden.

Es SOLLTEN Mechanismen zur Erkennung und Abwehr von hochvolumigen Angriffen, TCP-State-Exhaustion-Angriffen und Angriffen auf Applikationsebene implementiert sein.

Alle Fernwartungsvorgänge SOLLTEN protokolliert werden.

OPS.1.2.5.A21 Erstellung eines Notfallplans für den Ausfall der Fernwartung (S)

Es SOLLTE ein Konzept entwickelt werden, wie die Folgen eines Ausfalls von Fernwartungskomponenten minimiert werden können. Dieses SOLLTE festhalten, wie im Falle eines Ausfalls zu reagieren ist. Durch den Notfallplan SOLLTE sichergestellt sein, dass Störungen, Schäden und Folgeschäden minimiert werden. Außerdem SOLLTE festgelegt werden, wie eine zeitnahe Wiederherstellung des Normalbetriebs erfolgen kann.

OPS.1.2.5.A24 Absicherung integrierter Fernwartungssysteme (S)

Bei der Beschaffung von neuen IT-Systemen SOLLTE geprüft werden, ob diese IT-Systeme oder einzelne Komponenten der IT-Systeme über Funktionen zur Fernwartung verfügen. Werden diese Funktionen nicht verwendet, SOLLTEN sie deaktiviert werden. Die Funktionen SOLLTEN ebenfalls deaktiviert werden, wenn sie 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 Fernwartungsfunktionen SOLLTEN nur aus einem getrennten Managementnetz erreichbar sein.

OPS.1.2.5.A25 Entkopplung der Kommunikation bei der Fernwartung (S)

Direkte Fernwartungszugriffe von einem Fernwartungs-Client außerhalb der Managementnetze auf ein IT-System SOLLTEN vermieden werden. Ist ein solcher Zugriff notwendig, SOLLTE die Kommunikation entkoppelt werden. Dazu SOLLTEN Sprungserver verwendet werden. Der Zugriff auf Sprungserver SOLLTE nur von vertrauenswürdigen IT-Systemen aus möglich sein.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.2.5.A14 Dedizierte Clients und Konten bei der Fernwartung (H)

Zur Fernwartung SOLLTEN IT-Systeme eingesetzt werden, die ausschließlich zur Administration von anderen IT-Systemen dienen. Alle weiteren Funktionen auf diesen IT-Systemen SOLLTEN deaktiviert werden. Die Netzkommunikation der Administrationssysteme SOLLTE so eingeschränkt werden, dass nur Verbindungen zu IT-Systemen möglich sind, die administriert werden sollen.

Für Fernwartungszugänge SOLLTEN dedizierte Konten verwendet werden.

OPS.1.2.5.A22 Redundante Kommunikationsverbindungen (H)

Für Fernwartungszugänge SOLLTEN redundante Kommunikationsverbindungen eingerichtet werden. Die Institution SOLLTE Anbindungen zum Out-Of-Band-Management vorhalten.

OPS.1.2.5.A23 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Bundesamt für Sicherheit in der Informationstechnik beschreibt in seiner Veröffentlichung „Grundregeln zur Absicherung von Fernwartungszugängen“, wie Fernwartungszugänge sicher betrieben werden können.

Das Bundesamt für Sicherheit in der Informationstechnik beschreibt in seiner Veröffentlichung „Fernwartung im industriellen Umfeld“ wie Fernwartungszugänge im Industrieumfeld sicher betrieben werden können.