Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein OPS.1.2.5 Fernwartung

1. Einleitung

Mit dem Begriff Fernwartung wird 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 auf unterschiedliche Weise geschehen. Bei der Fernwartung von Clients werden oft die Tastatur- und Maussignale vom IT-System eines Administrators an ein entferntes IT-System übertragen. Das entfernte IT-System überträgt die Bildschirmausgabe an das IT-System des Administrators. Der Administrator führt Aktionen auf dem entfernten IT-System aus, als wenn er selbst vor Ort wäre (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 zum Administrator übertragen. Der Administrator erteilt einem Benutzer vor Ort Anweisungen, die von ihm ausgeführt und vom Administrator 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 Administratoren 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.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins OPS.1.2.5 *Fernwartung* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein OPS.1.2.5 Fernwartung

OPS.1.2.5.M1 Planung des Einsatzes der Fernwartung (B)

Der Einsatz der Fernwartung muss an die Institution angepasst und bedarfsgerecht hinsichtlich technischer und organisatorischer Aspekte geplant werden. Es sollten mindestens die folgenden Aspekte im Rahmen der Einsatzplanung betrachtet werden:

- Soll die Fernwartung In-Band (also innerhalb des normalen IT-Netzes) oder Out-Band (also über ein dediziertes Administrationsnetz) stattfinden? Bei erhöhtem Schutzbedarf empfiehlt es sich, die Fernwartung aus einem dedizierten Administrationsnetz durchzuführen.
- Welche Schnittstellen und Protokolle sollen verwendet werden?
- Welche gesetzlichen und internen Regelungen sind zu berücksichtigen?
- Erfolgt die Fernwartung durch Dienstleister?
- Dürfen Online-Dienste zur Fernwartung genutzt werden?
- Welche Aufgabenverteilung innerhalb der Institution muss beim Einsatz der Fernwartung erfolgen?
- Welche Anforderungen aus der Netzseparierung sind zu beachten?

Je genauer die Rahmenbedingungen bekannt und je präziser die Vorgaben formuliert sind, desto einfacher werden die nächsten Konzeptionierungs- und Umsetzungsschritte der Fernwartung.

OPS.1.2.5.M2 Sicherer Verbindungsaufbau bei der Fernwartung von Clients (B)

Wird per Fernwartung auf Clients zugegriffen, muss der Benutzer des IT-Systems diesem Zugriff explizit zustimmen. Dies kann dadurch erfolgen, dass der Benutzer des Systems die Fernwartungsverbindung selbst initiiert. Alternativ kann der entfernte Administator die Verbindung starten. Der Zugriff auf das IT-System darf dann jedoch erst möglich sein, wenn er explizit durch den Benutzer freigegeben wurde, z. B. über eine entsprechende Bestätigung am System.

Das Wartungspersonal muss sich zu Beginn der Wartung authentisieren. Wird die Verbindung zur Fernwartungsstelle auf irgendeine Weise unterbrochen, so muss eine eventuell vorhandene Session beendet werden und der Zugriff auf das System erneut initiiert werden.

OPS.1.2.5.M3 Absicherung der Schnittstellen zur Fernwartung (B)

Die Kommunikationsschnittstellen und möglichen Zugänge für einen Verbindungsaufbau von außen sind auf das notwendige Maß, entsprechend der verwendeten Betriebssysteme und weiteren damit in Verbindung stehenden Hardware- und Software-Komponenten, zu beschränken. Ebenso müssen alle Kommunikationsverbindungen der Fernwartung nach vollzogenem Fernzugriff getrennt werden. Notwendige Ports für die Fernwartung müssen abgesichert werden. Zum Beispiel können die zur Verfügung stehenden Ports mit Hilfe eines Firewall-Portals und hinterlegten Firewall-Regel nach erfolgreicher Authentisierung eines berechtigten Administrators geöffnet werden.

Es müssen unter Berücksichtigung des Schutzbedarfes des jeweiligen IT-Systems, der Anwendung bzw. der damit verbundenen Netzseparierung sichere Mechanismen zur Authentisierung eingesetzt werden. Wird für die Kommunikation kein eigenständiges Administrationsnetz verwendet, sollte eine

Alternative mit identischen Sicherheitsmerkmalen verwendet werden. Der erlaubte Personenkreis für einen Verbindungsaufbau sollte nach dem Minimalprinzip eingeschränkt werden.

Wichtig ist, dass bei den Kommunikationsverbindungen und dem Verbindungsaufbau bei der Fernwartung folgende Punkte sichergestellt werden:

- Vertraulichkeit der übertragenen Daten: Die Vertraulichkeit der übertragenden Daten muss durch eine ausreichende sichere Verschlüsselung sichergestellt werden.
- Integrität der übertragenen Daten: Die eingesetzten Übertragungsprotokolle müssen eine zufällige Veränderung übertragener Daten erkennen und beheben.
- Verfügbarkeit der Fernwartung: Falls zeitliche Verzögerungen bei der Fernwartung nur schwer zu tolerieren sind, sollten redundante Übertragungswege zur Verfügung gestellt werden.
- Nachvollziehbarkeit der Datenübertragung: Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, die nachträglich feststellen lassen, welche Daten wann und an wen übertragen wurden.
- Datenempfang: Ist es für die Fernwartung von Bedeutung, ob Daten korrekt empfangen wurden, können Quittierungsmechanismen eingesetzt werden, aus denen hervorgeht, ob der Empfänger die Daten korrekt empfangen hat.

OPS.1.2.5.M4 ENTFALLEN (B)

Die zugehörige Anforderung ist entfallen.

OPS.1.2.5.M5 Einsatz von Online-Diensten (S)

In vielen Situationen werden Online-Dienste zur Fernwartung eingesetzt, bei der die Verbindung über die Server eines Dritten hergestellt wird. Dabei verbindet sich das IT-System des Administrators und das IT-System, das ferngewartet werden soll, mit einem Dienstanbieter im Internet. Für die Beteiligten ist nicht erkennbar, was mit übertragenen Informationen beim Diensteanbieter passiert bzw. welche Eingriffsmöglichkeiten dort bestehen. Es könnten Inhalte mitgeschnitten oder auch manipuliert werden. Dies gilt z. B. auch für Tastatureingaben (z. B. Passwörter).

Werden Online-Dienste genutzt, entstehen aber sicherheitstechnische Risiken. Online-Dienste sollten deswegen nur dann eingesetzt werden, wenn eine andere Lösung nur mit unverhältnismäßigem Aufwand umsetzbar ist. Die Institution sollte genau festlegen, welche Systeme unter welchen Bedingungen mit Online-Diensten ferngewartet werden dürfen. Außerdem sollte ein Online-Dienst gewählt werden, bei dem die Daten Ende-zu-Ende verschlüsselt übertragen werden.

Oft starten die Clients der Fernwartenden den Dienst automatisch und verbinden sich mit dem Online-Dienst. Ist dies der Fall, kann jeder, der die Zugangsdaten kennt (oft nur eine ID und PIN) auf die Clients zugreifen. Es sollte verboten werden, dass Clients automatisch eine Verbindung zu Online-Diensten aufbauen können, dies sollte auch technisch verhindert werden.

Der Vorteil von Online-Diensten besteht darin, dass z. B. in einem Notfall eine Fernwartung schnell initiiert werden kann, weil bei den Beteiligten nur ein geringer Aufwand erforderlich ist. In diesem Fall muss allerdings vorab genau geregelt werden, in welchen Fällen und unter welchen Bedingungen Online-Dienste zum Fernzugriff erlaubt sind. Diese sind zu dokumentieren und mit dem ISB und dem Datenschutzbeauftragten der Institution vorab abzustimmen.

Die Regelungen sollten z. B. folgende Punkte umfassen:

- Es sollte festgelegt werden, in welchen Fällen eine Fernwartung über Online-Dienste erlaubt ist. Beispielsweise kann es notwendig sein, bei definierten Notfällen oder um unmittelbare Gefahr für den Dienstbetrieb abzuwenden, auf die Fernwartung über Online-Dienste zurückzugreifen.
- Es muss geregelt werden, wie und von wem die Nutzung von Online-Diensten autorisiert wird. Dabei sollten für den Einzelfall die existierenden Meldewege eingehalten werden.

- Ein automatischer Verbindungsaufbau sollte untersagt werden. Die Verbindung muss im Einzelfall vom fernzuwartenden IT-System freigegeben werden.
- Für jede Verbindung sind neue Zugangsdaten zu generieren (z. B. neue PIN).
- Die Zugangsdaten dürfen nicht in Klartext über unsichere Netze übermittelt werden (z. B. nur mündlich, verschlüsselt).
- In einer Verbindung über einen Online-Dienst dürfen keine Passwörter oder andere vertrauliche Informationen dargestellt oder lokal eingegeben werden. Mit einer "Whitelist" kann beschrieben werden, welche Informationen übertragen werden dürfen.

OPS.1.2.5.M6 Erstellung einer Richtlinie für die Fernwartung (S)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution sollten die wesentlichen Kernaspekte für die Fernwartung konkretisiert werden. Dabei sollten insbesondere die Punkte berücksichtigt werden, zu denen bereits eine Planung stattgefunden hat (siehe OPS.1.2.5.M1 *Planung des Einsatzes der Fernwartung*).

Die Richtlinie muss allen Zuständigen, die an der Konzeption, dem Aufbau und dem Betrieb sowie der Aussonderung beteiligt sind, bekannt sein und die Grundlage für deren Arbeit bilden können. Die Umsetzung der in der Richtlinie geforderten Inhalte sollte regelmäßig überprüft werden und die Ergebnisse sind anschließend sinnvoll zu dokumentieren. Die Vorgaben innerhalb der Richtlinie sollten stringent sein, um spätere Risikoeinschätzungen oder Risikoübernahmen durchführen zu können. Wird kryptographische Kommunikation für die Fernwartung benötigt, müssen die Anforderungen des Bausteins *CON.1 Kryptokonzept* berücksichtigt werden.

OPS.1.2.5.M7 Dokumentation bei der Fernwartung (S)

Es muss eine aktuelle Dokumentation zur Fernwartung vorliegen. Vorhandene Dritte sollten, mit Hilfe der Fernwartungsdokumentation, zu jeder Zeit die Aufgaben und Prozesse, übernehmen können.

Da die Dokumente, z. B. Arbeitsanweisungen für die Initiierung eines Fernzugriffs, meist vertrauliche Informationen und Daten beinhalten, müssen sie an geeigneten Orten gesichert abgelegt werden und vor unbefugtem Zugriff geschützt sein. Die Dokumente müssen im Rahmen des Notfallmanagements zur Verfügung stehen. Sämtliche Fernzugriffsmöglichkeiten müssen erfasst und dokumentiert sein. Im Asset-Management der Institution sollten die Systeme und deren Schnittstellen für die Fernadministration hinterlegt sein. Für das Notfallmanagement und für den Wiederanlaufplan sollten die internen und externen Ansprechpartner der Systeme hinterlegt werden.

Die allgemeine Dokumentation der administrativen Prozesse für die verschiedenen IT-Komponenten sollte in Form von Betriebshandbüchern erfolgen. Im Betriebshandbuch für das jeweilige System, das aus der Ferne administriert werden soll, muss ein Hinweis enthalten sein, von welchem System aus, mit welchen Rechten und durch welche Organisationseinheit hierauf zugegriffen werden darf.

OPS.1.2.5.M8 Sichere Protokolle bei der Fernwartung (S)

Es sollten ausschließlich aktuelle und als sicher eingestufte Kommunikationsprotokolle zur Fernwartung eingesetzt werden. Die Kommunikation sollte verschlüsselt werden. Die Empfehlungen des BSI aus der technischen Richtlinie "Kryptographische Verfahren: Empfehlungen und Schlüssellängen" [TR02102] sollten bei der Auswahl der Protokolle und Algorithmen beachtet werden.

Die Administration mittels Tunnel kann beispielsweise durch einen SSH-Tunnel, TLS-Tunnel oder IPSec-Tunnel abgesichert erfolgen. Es sollte ausgehend vom Schutzbedarf der Institution eine angemessene Tunnelmethode ausgewählt werden. Diese muss natürlich von den eingesetzten IT-Systemen auch unterstützt werden. Zu beachten ist, das die verwendeten Protokolle ausreichend von der Fachwelt untersucht wurden und als sicher betrachtet werden.

Für die Verwendung der folgenden Protokolle empfiehlt sich die Verwendung der jeweiligen Versionen:

- Einsatz von SSH in der Version 2

- Gebrauch von TLS ab Version 1.2 mit PFS
- Nutzung von IPsec mit IKEv2 und idealerweise Zertifikaten

OPS.1.2.5.M9 Auswahl und Beschaffung geeigneter Fernwartungswerkzeuge (S)

Es liegen keine Hinweise zur Umsetzung vor. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.bund.de entgegengenommen.

OPS.1.2.5.M10 Verwaltung der Fernwartungswerkzeuge (S)

Da Fernwartungswerkzeuge eine Vielfalt unterschiedlicher Funktionen ermöglichen, müssen organisatorische Verwaltungsprozesse zum Umgang mit den ausgewählten Werkzeugen etabliert werden. Es muss eine Bedienungsanleitung für den geeigneten Umgang mit den Fernwartungswerkzeugen für den IT-Betrieb vorliegen. Musterabläufe für die passive und die aktive Fernwartung müssen für die Nutzung innerhalb der Institution erstellt und kommuniziert werden. Um mögliche Sicherheitslücken, resultierend aus Fehlkonfigurationen und Bedienungsproblemen, zu minimieren, muss der IT-Betrieb im Umgang mit den Fernwartungswerkzeugen sensibilisiert und geschult werden. Es muss ein Zuständiger benannt werden, der als Ansprechpartner für alle fachlichen Fragen zu den Fernwartungswerkzeugen dient.

Vorgaben für die Prozesse der Fernwartung

- Für den Betrieb von Fernwartungswerkzeugen sind Vorgaben und Abläufe festzulegen. Zum Beispiel sollte festgelegt werden, wer auf die Werkzeuge zugreifen darf und wo Änderungen damit durchgeführt werden dürfen. Dies sollte in Form eines Prozessschaubildes dokumentiert werden.
- Die Fernwartungswerkzeuge müssen in den Prozess der Fernwartung selbst und in das Patch- und Änderungsmanagement eingegliedert werden, sofern diese nicht bereits Teil des Betriebssystems sind.

OPS.1.2.5.M11 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

OPS.1.2.5.M12 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

OPS.1.2.5.M13 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

OPS.1.2.5.M14 Dedizierte Systeme bei der Fernwartung (H)

Zur Fernwartung sollten IT-Systeme eingesetzt werden, die ausschließlich zur Administration von anderen IT-Systemen dienen. Alle weiteren Funktionen und Dienste sollten deaktiviert werden. Insbesondere sollten die Fernwartungs-Systeme nicht als normale (Büro-)Arbeitsplatzrechner eingesetzt werden. Durch die Umsetzung des Minimalprinzips wird automatisch auch die mögliche Angriffsfläche reduziert, die von Angreifern für Kompromittierungen genutzt werden könnten. Die dedizierten IT-Systeme stellen ihre Leistung und Ressourcen (z. B. RAM, CPU-Kapazität, Festplattenplatz) somit nur dem notwendigen Einsatzzweck zur Verfügung. Die IT-Systeme der Fernwartung sollten sicher konfiguriert sowie mit den aktuellsten Betriebssystem- und Anwendungssoftwareversionen betrieben werden. Nicht benötigte Netzverbindungen sollten unterbunden werden.

OPS.1.2.5.M15 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

OPS.1.2.5.M16 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

OPS.1.2.5.M17 Authentisierungsmechanismen bei der Fernwartung (S)

Zur Fernwartung werden dem Schutzbedarf angemessene Mechanismen zur Identifikation und Authentisierung benötigt. Es sollte Zwei-Faktor-Authentisierung verwendet werden.

Die Auswahl der Authentisierungsmethode und die Gründe, die zu der Auswahl geführt haben, sollten dokumentiert werden. Bestehende Authentisierungsmechanismen der Institution dürfen durch die Fernwartung nicht umgangen werden. Zur Erleichterung der Anmeldung bei der Fernwartung empfiehlt es sich, diese in ein Identitäts- und Berechtigungsmanagement und dessen Infrastruktur zu integrieren.

OPS.1.2.5.M18 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

OPS.1.2.5.M19 Fernwartung durch Dritte (S)

Es kann verschiedene Gründe geben, warum die Fernwartung durch Dritte durchgeführt werden soll. Beispielsweise kann die Fernwartung zu den vereinbarten Serviceleistungen von Geräteherstellern gehören. Es können auch intern die erforderlichen Ressourcen oder das Fachwissen fehlen.

Fernwartung durch Dritte ist besonders kritisch. Sollte sie im Einzelfall notwendig sein, sind folgende Punkte zu beachten:

- Alle durchgeführten Änderungen (z. B. der Konfigurationseinstellungen) sollten dokumentiert werden. Diese Dokumentation muss der ferngewarteten Institution übergeben werden.
- Wenn dies technisch möglich ist, sollten alle Tätigkeiten während der Administration von Dritten durch eigene IT-Experten beobachtet werden. Beispielsweise können bei der Fernadministration eines Clients über eine graphische Benutzeroberfläche oft alle Ein- und Ausgaben am zu wartenden IT-System angezeigt und aufgezeichnet werden. Auch wenn Fernwartung durch Dritte genutzt wird, weil intern das Know-how oder die Kapazität nicht verfügbar ist, kann das externe Wartungspersonal nicht unbeaufsichtigt gelassen werden. Bei Unklarheiten über die Vorgänge sollte die Verbindung sofort unterbrochen bzw. auf betrachtenden Modus umgeschaltet werden. Danach können die Fragen geklärt werden.
- Wenn eine Fernwartung durch Dritte nicht überwacht wird, sollte sie im Normalbetrieb gesperrt sein und nur durch explizite Freigabe für eine genau definierte Zeitspannen aktiviert werden
- Es muss jederzeit die Möglichkeit geben, die Fernwartung lokal abzubrechen.
- Werden während der Wartung Daten oder Programme auf dem lokalen IT-System angelegt, so muss dies deutlich erkennbar und nachvollziehbar sein, z. B. darf dies nur in besonders markierten Verzeichnissen oder unter bestimmten Benutzer-Kennungen erfolgen.
- Alle Fernwartungsvorgänge müssen dokumentiert werden. Dabei ist zumindest Anfang und Ende der Fernwartung sowie die Beteiligten festzuhalten. Wenn auf dem gewarteten IT-System niemand die Fernzugriffe beobachten kann, müssen alle Tätigkeiten bei der Durchführung der Fernwartung auf dem zu wartenden IT-System protokolliert werden.
- Für das externe Wartungspersonal müssen vertragliche Regelungen getroffen worden sein, vor allem über die Geheimhaltung von Daten (Vertraulichkeitsvereinbarungen). Insbesondere ist festzulegen, dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden. Ebenso sind die Pflichten und Kompetenzen des externen Wartungspersonals sorgfältig festzulegen.

Bei höherem Schutzbedarf sollten außerdem vor der Auswahl eines Fernwartungspartners Informationen über dessen Zuverlässigkeit und weiterführende Informationen eingeholt werden. Im

Rahmen der betrieblichen, sicherheitstechnischen und datenschutzrechtlichen Vereinbarungen sowie der Zusammenarbeit in Notfällen sollten beispielsweise auch die Anforderungen an die zu erfüllenden Service Level Agreements (SLAs, Dienstgütevereinbarungen) übergeben werden. Darüber hinaus sollten Abstimmungen hinsichtlich der zu erfüllenden Netzsegmentierungs- und Separierungsvorgaben sowie die erwarteten Schutzmechanismen für die Clients und deren zugrundeliegende Betriebssysteme getroffen werden. Die Institution sollte mit dem Dienstleister vertraglich entsprechende Kontrollmechanismen festlegen.

In Bezug auf das Identitäts- und Berechtigungsmanagement gilt bei der Auswahl des Fernwartungsdienstleisters, dass dieser nie mehr Rechte erhalten darf, als er für die Erfüllung seiner Aufgaben unbedingt benötigt und das sich jeder Mitarbeiter des Dienstleisters über eine eindeutige personalisierte Benutzerkennung authentisieren muss.

Da die Institution als Dienstleistungsnehmer keinen direkten Einfluss auf die Arbeitsweise des Dienstleisters und dessen Personal besitzt, können sich durch mögliche Nachlässigkeiten oder Unzuverlässigkeiten unkontrollierbare Risiken ergeben. Um diese Risiken zu minimieren, sollten vertragliche Vereinbarungen zu mindestens den folgenden Themenfeldern benannt werden:

- Gemeinsames Risikomanagement durch die enge Verzahnung der Fernwartungssysteme des Dienstleisters mit den Systemen der Institution,
- Sicherheitsvorfallerkennung und -behandlung,
- gemeinsames Notfallmanagement inklusive der Benennung der Business-Impact-Analyse-Werte (BIA-Werte),
- eine Vertraulichkeitsvereinbarung,
- Festlegung der Kompetenzen und Pflichten,
- Festlegungen bezüglich Backup und Archivierungsanforderungen,
- eine genaue Beschreibung, wie die IT-Systeme des Dienstleisters geschützt werden,
- Festlegungen rund um die Möglichkeit der Auditierung,
- Festlegungen zum Zwecke der Einbindung in die Überwachungs- und Protokollierungsinfrastruktur der Institutionsstandorte,
- Übergabe bzw. bestätigte Vernichtung (Vernichtungserklärung) der Backup- und Archivierungsdaten im Rahmen der Fernwartung nach Vertragsbeendigung.

Weitere Informationen für den Betrieb der Fernwartung durch Dritte sind in den Bausteinen OPS.2.1 *Outsourcing für Kunden* und OPS.3.1 *Outsourcing für Dienstleister* beschrieben.

OPS.1.2.5.M20 Betrieb der Fernwartung (S)

Es liegen keine Hinweise zur Umsetzung vor. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.de entgegengenommen.

OPS.1.2.5.M21 Erstellung eines Notfallplans für den Ausfall der Fernwartung (S)

Im Rahmen der Notfallvorsorge sollte ein Konzept entwickelt werden, wie die Folgen eines Ausfalls von Fernwartungskomponenten minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind. Durch den Notfallplan sollte sichergestellt sein, dass Störungen, Schäden und Folgeschäden minimiert werden sowie eine zeitnahe Wiederherstellung des Normalbetriebs erfolgt. Bei Hochverfügbarkeit sollte die Infrastruktur der Fernwartung mittels einer Business-Impact-Analyse geprüft werden.

Weitere Aspekte der Notfallplanung werden im Baustein im Baustein DER.4 *Notfallmanagement* behandelt.

OPS.1.2.5.M22 Redundante Kommunikationsverbindungen (H)

Für den Schutz der Kommunikationsnetze der Fernwartung bei Hochverfügbarkeitsanforderungen sollten redundante Verbindungs- bzw. Kommunikationsnetze eingerichtet werden. Es sollten geregelt werden, ob hierfür externe Telekommunikationsnetze genutzt werden sollen, beispielsweise Mobilfunk.

Die internen IT-Systeme der Institution sollten neben den etablierten produktiven Wegen zusätzlich über ein nicht produktiv genutztes Fallback-Zugangsnetz erreichbar sein. Der Fallback-Zugang könnte zum Beispiel über eine DSL- oder LTE-Verbindung realisiert sein beziehungsweise durch eine Festnetzverbindung.

OPS.1.2.5.M23 ENTFALLEN (H)

Die zugehörige Anforderung ist entfallen.

OPS.1.2.5.M24 Absicherung integrierter Fernwartungssysteme (S)

Viele IT-Systeme enthalten Komponenten, die eigene Fernwartungsfunktionen zur Verfügung stellen (beispielsweise enthalten viele Prozessoren eigene Fernwartungsfunktionen, die vom Betriebssystem des IT-Systems unbemerkt arbeiten). Häufig sind diese Funktionen schlecht dokumentiert und nicht ohne Weiteres deaktivierbar.

Bevor neue IT-Systeme beschafft werden, sollte geprüft werden, ob sie Fernwartungsfunktionen enthalten. Falls solche Funktionen nicht verwendet werden, sollten sie soweit wie möglich abgeschaltet werden. Dabei sollte jedoch nur auf Verfahren zurückgegriffen werden, die keine unerwarteten oder negativen Auswirkungen auf andere Funktionen des betroffenen Systems haben. Fernwartungsfunktionen sollten ebenfalls abgeschaltet werden, wenn sie durch bekannt gewordene Sicherheitslücken angegriffen werden können.

Falls integrierte Fernwartungsfunktionen verwendet werden, sollte der Zugriff darauf nur aus einem separaten Managementnetz möglich sein. Der Zugriff aus anderen Netzen und von Systemen, die nicht zur Fernwartung dienen, sollte verhindert werden. Falls dies nicht durch native Funktionen der Fernwartungskomponente möglich ist, sollten dazu Maßnahmen auf Netzebene ergriffen werden.

OPS.1.2.5.M25 Entkopplung der Kommunikation bei der Fernwartung (S)

Es liegen keine Hinweise zur Umsetzung vor. Anregungen aus der Praxis werden gerne unter grundschutz@bsi.bund.de entgegengenommen.

3. Weiterführende Informationen

3.1. Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2. Quellenverweise

[TR02102] Kryptographische Verfahren: Empfehlungen und Schlüssellängen: BSI TR-02102, Bundesamt für Sicherheit in der Informationstechnik (BSI), Januar 2018, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html , zuletzt abgerufen am 13.09.2018