Bundesamt
für Sicherheit in der
Informationstechnik

IND.3.2 Fernwartung im industriellen Umfeld

1. Beschreibung

1.1. Einleitung

Die Betriebstechnik (OT) einer Institution besitzt häufig eine dezentrale Infrastruktur. Verschiedene Bereiche der OT können räumlich weit auseinanderliegen. Zudem bestehen Industrial-Control-Systeme (ICS) meist aus einer Vielzahl von Produkten verschiedener herstellenden Unternehmen, d. h. aus unterschiedlichen ICS-Komponenten und IT-Systemen für OT-Anwendungen. Daher benötigt die Betriebstechnik einer Institution in der Regel zahlreiche Fernwartungszugänge.

Diese Fernwartungszugänge sind häufig Einzellösungen in Form individuell zusammengestellter Hard- und Softwarekomponenten. Infolgedessen wird eine Vielzahl unterschiedlicher Techniken für die OT-Fernwartung eingesetzt. Die Lebenszyklen der Fernwartungslösungen entsprechen dabei meist denjenigen der Produkte, auf die zugegriffen wird, d. h. die Fernwartungslösungen für OT werden unter Umständen wesentlich länger eingesetzt als dies in der IT üblich ist. Verschiedenste Zugänge, Dienste und Schnittstellen sind parallel vorhanden. Die Schnittstellen kommunizieren mittels unterschiedlichster Protokolle.

Manche Anlagenteile in der OT werden auch als geschlossene Einheit von den herstellenden Unternehmen realisiert (sogenannte Package Units). Diese Anlagenteile enthalten häufig mehrere dezentrale Zugänge für die Fernwartung, die die herstellenden Unternehmen von vornherein für ihren eigenen Zugriff betriebsbereit integriert haben.

Fernwartungszugänge im industriellen Umfeld werden in der Regel vom OT-Betrieb und Wartungspersonal genutzt, um OT-Komponenten zu konfigurieren, zu kontrollieren, zu warten und zu reparieren. Nur in Ausnahmefällen, z. B. bei Störungen, nutzen auch weitere Mitarbeitende OT-Fernwartungszugänge.

Auf OT-Komponenten wird via Fernwartung von verschiedenen Institutionen aus zugegriffen. Nicht nur das interne Personal des Betreibenden, sondern auch externes Personal von herstellenden Unternehmen, Integratoren und Dienstleistenden nutzt Fernwartungszugänge.

Grundsätzlich erfolgt ein Fernwartungszugriff in dasjenige Sicherheitssegment eines OT-Netzes, in dem der Fernwartungsdienst bereitgestellt wird. Der Fernwartungsdienst kommuniziert dann aus diesem Segment heraus mit dem zu wartenden Zielsystem, z. B. mit einer ICS-Komponente.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit der Fernwartung im industriellen Umfeld zu gewährleisten.

1.3. Abgrenzung und Modellierung

Der Baustein IND.3.2 *Fernwartung im industriellen Umfeld* ist einmal auf die gesamte OT einer Institution anzuwenden, sobald diese Möglichkeiten zur Fernwartung enthält. Von den jeweiligen Einsatzgebieten der ICS ist abhängig, ob weitere Anforderungen an die Fernwartung im industriellen Umfeld definiert werden müssen, die in diesem Baustein nicht allgemeingültig aufgeführt werden können. Je nach Einsatzgebiet können auch die Maßnahmen unterschiedlich sein, die umgesetzt werden sollten, um die Anforderungen zu erfüllen.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt

- die spezifischen Aspekte der OT-Fernwartung, die über die allgemeine Verwaltung von Netzkomponenten und IT-Systemen per Fernwartung hinausgehen sowie
- die spezifischen Aspekte der OT-Fernwartung, die von der allgemeinen Verwaltung von Netzkomponenten und IT-Systemen per Fernwartung abweichen.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- die allgemeine Verwaltung von Netzkomponenten und IT-Systemen per Fernwartung durch den IT-Betrieb in der Büro- und Gebäude-IT (siehe OPS.1.2.5 *Fernwartung*) (Die diesbezüglichen Anforderungen sind grundsätzlich auch in der OT zu erfüllen.)
- die allgemeinen Aspekte zu Netzarchitektur und -design, sowie zu der Segmentierung (siehe NET.1.1 *Netzarchitektur und -design*)
- die individuellen Aspekte der Hard- und Software-Komponenten, aus denen die jeweilige Fernwartungslösung besteht, z. B. Netzkomponenten, Server- und Clientsysteme, OT-Anwendungen (Hier sind die jeweils zutreffenden Bausteine zu modellieren.)
- die allgemeinen Aspekte der Protokollierung (siehe OPS.1.1.5 *Protokollierung*)
- die allgemeinen Aspekte des Outsourcings (siehe OPS.2.3 *Nutzung von Outsourcing*)
- die allgemeinen Aspekte cloudbasierter Fernwartungslösungen (siehe OPS.2.2 *Cloud-Nutzung*)
- die allgemeinen Aspekte webbasierter Fernwartungslösungen (siehe APP.3.1 *Webanwendungen und Webservices*)
- die allgemeinen Aspekte der Absicherung von ICS auf Bedienebene (siehe IND.1 *Prozessleit- und Automatisierungstechnik* und IND.2.7 *Safety Instrumented Systems*)

Dieser Baustein behandelt **nicht**

- die Beobachtung und Bedienung von ICS auf Prozessebene sowie
- steuernde Zugriffe per Fernwartung auf ICS, z. B. Anlaufen oder Stoppen von Anlagen. Solche Zugriffe können grundsätzlich Personen- und Sachschäden vor Ort verursachen!

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 IND.3.2 *Fernwartung im industriellen Umfeld* von besonderer Bedeutung.

2.1. Unvollständig dokumentierte Fernwartungszugänge in der OT

Die Fernwartungszugänge in der OT einer Institution sind in der Regel zahlreich und vielfältig. Darüber hinaus greift eine große Anzahl von internen und externen Personen darauf zu. Die Verwaltung von Fernwartungszugängen im industriellen Umfeld ist daher grundsätzlich unübersichtlich und fehleranfällig. Es besteht eine größere Gefahr als in der Büro- und Gebäude-IT, dass die diversen Zugänge unzureichend erfasst und dokumentiert werden, d. h. nicht überprüfbar sind.

Wenn unbekannte, offene OT-Fernwartungszugänge nicht dokumentiert sind, können die Betreibenden Zugriffe nicht unterbinden. In der Folge können unautorisierte Benutzende die physischen Abläufe eines ICS direkt beeinflussen, was z. B. zu Fehlverhalten einzelner Komponenten, zum Stillstand einer ganzen Produktionsanlage bis hin zu Gefahren für Leib und Leben von Mitarbeitenden vor Ort führen kann. Werden z. B. Anlagen inklusive dezentraler Komponenten für die Fernwartung als Gesamtsystem (Package Unit) vom herstellenden Unternehmen realisiert, unterliegen diese zunächst keiner ausreichenden Kontrolle durch die Betreibenden. Diese müssen jede OT-Fernwartungskomponente einzeln erfassen und häufig aktiv umkonfigurieren.

Wenn einige OT-Fernwartungszugänge z. B. nur dezentral erfasst und dokumentiert werden, dann besteht auch die Gefahr, dass notwendige Änderungen an einzelnen Zugängen unterbleiben oder durchgeführte Änderungen nicht nachvollziehbar sind.

2.2. Unzureichende Verfügbarkeit durch Abhängigkeiten von der Büro- und Gebäude-IT

ICS sind in Teilen auf einen vollständig unterbrechungsfreien Informationsfluss angewiesen. Dies gilt insbesondere für sämtliche Echtzeit-Datenströme. Bereits sehr kurze Unterbrechungen der Verfügbarkeit von Daten, die in der Büro- und Gebäude-IT toleriert werden können, können in einem ICS kritisch sein. Darüber hinaus können durch Abhängigkeiten von Netzen, Diensten oder IT-Systemen Sicherheitslücken entstehen. Dies wird häufig bei der Planung übersehen, wenn die OT und die Büro- und Gebäude-IT einer Institution miteinander kommunizieren.

Wenn Abhängigkeiten zwischen OT und Büro- und Gebäude-IT nicht beachtet und infolgedessen Sicherheitslücken nicht geschlossen werden, dann können Sicherheitsvorfälle schnell auf die gesamte OT übergreifen.

Wenn zentrale Komponenten und Dienste der Büro- und Gebäude-IT für die Fernwartung der OT genutzt werden (übergreifende Administration), dann kann es auch zu Abstimmungsfehlern zwischen Büro- und Gebäude-IT sowie OT kommen. In der Folge kann die Behebung kritischer Fehler in den ICS der OT verzögert werden. Ein Beispiel ist ein zentrales VPN-Gateway für den Fernzugriff, das durch eine Organisationseinheit außerhalb der OT bereitgestellt und nicht entsprechend abgestimmt betrieben wird, sodass es bei Bedarf nicht schnell genug zur Verfügung steht. Der Stillstand einer Anlage kann sich dann erheblich verlängern.

2.3. Unzureichende Regelungen für die Nutzung von OT-Fernwartungszugängen

OT-Fernwartungszugänge haben einen sehr großen potentiellen Benutzendenkreis außerhalb der betreibenden Institution. Gleichzeitig ist die lückenlose Verfügbarkeit von Echtzeitdaten in einem ICS unerlässlich, während die Verfügbarkeit von Daten der Büro- und Gebäude-IT in der Regel etwas weniger zeitkritisch ist. Allgemeine Regelungen, wie Fernwartungszugänge für die Büro- und Gebäude-IT genutzt werden, sind für die OT häufig unpassend oder lassen zu viel Spielraum.

Wenn die Nutzung von OT-Fernwartungszugängen nur unzureichend vertraglich geregelt ist, dann fehlen klare Vorgaben, wie der Benutzendenkreis jedes einzelnen Zugangs einzuschränken ist. Die Betreibenden können dann nicht kontrollieren, wer ihre OT-Fernwartungszugänge nutzt. So können z. B. Zugangsdaten bei Integratoren, Herstellenden und Wartungsdienstleistenden an Benutzende weitergegeben werden, die den Betreibenden unbekannt sind. Dies ist für ein ICS nicht tolerierbar.

Wenn restriktive Nutzungsregelungen speziell für die OT fehlen, dann können die Betreibenden auch nicht angemessen kontrollieren, wie OT-Fernwartungszugänge genutzt werden. Im Falle eines (Sicherheits-)Vorfalls wird dann z. B. die (forensische) Analyse erschwert, weil Ursachen nicht schnell genug erkannt werden können. Dies kann kostenintensive Produktionsstillstände verlängern.

Wenn OT-Fernwartungszugänge gemeinsam mit oder von der Büro- und Gebäude-IT bereitgestellt und betrieben werden und diese gemeinsame Nutzung der Hard- oder Software des Zugangs nicht eindeutig geregelt ist, dann können inkonsistente Konfigurationen auftreten. Diese erfüllen dann nur die Sicherheitsanforderungen der Büro- und Gebäude-IT, nicht jedoch abweichende oder zusätzliche Sicherheitsanforderungen der OT.

2.4. Unzureichende menschliche Kontrolle über OT-Fernwartungssitzungen

Die Daten und Konfigurationseinstellungen innerhalb eines ICS sowie Personen, Sachen und Produktionsprozesse vor Ort können durch sämtliche Zugriffe aus anderen Zonen gefährdet sein, die nicht oder nur unzureichend durch internes Personal vor Ort kontrolliert werden. Insbesondere das Personal externer Wartungsdienstleistenden, Integratoren und herstellenden Unternehmen verfügt zwar über die notwendige Spezialkenntnis der zu wartenden Anlage, Maschine oder Komponente, weiß jedoch nicht, welche schädlichen Auswirkungen die konkrete Fernwartungssitzung im Gesamtsystem haben kann.

Wenn die Verläufe und Inhalte von OT-Fernwartungssitzungen von den Betreibenden nicht angemessen kontrolliert werden können, dann können Konfigurationsfehler mit hohem Gefährdungspotential sowie unabsichtliches oder absichtliches Fehlverhalten des Wartungspersonals nicht schnell genug erkannt und nachvollzogen werden. Dann sind Ausfälle oder Manipulationen von Echtzeit-Datenströmen möglich oder Schadsoftware kann sich unbemerkt in der gesamten OT ausbreiten. Schäden an Leib und Leben des Bedienungspersonals vor Ort oder hohe finanzielle Schäden durch Produktionsausfälle bis zur Zerstörung ganzer Anlagen können dann die Folge sein. Auch die Offenlegung von Betriebsgeheimnissen ist möglich. Zudem kann die Integrität der hergestellten Produkte beeinträchtigt werden, z. B. durch Manipulation von Rezepten, sodass Ausschuss produziert wird, der unter Umständen schwer zu erkennen ist. Wenn mangelhafte Produkte nicht als solche erkannt werden, dann kann dies die Reputation der Institution schädigen.

Ein Beispiel sind dezentrale OT-Fernwartungskomponenten innerhalb von Anlagen, die als Gesamtsystem von herstellenden Unternehmen realisiert werden (Package Units). Diese Fernwartungszugänge sind häufig so konstruiert, dass die herstellenden Unternehmen zu jeder Zeit auf die Anlage zugreifen können. Geschieht dies ohne Abstimmung mit dem Personal des oder der Betreibenden, dann können z. B. Gefahrensituationen im aktuellen Produktionsablauf entstehen.

2.5. Direkte IP-basierte Zugriffsmöglichkeiten auf ICS aus unsicheren Zonen

Die Daten innerhalb eines ICS sowie Personen, Sachen und Produktionsprozesse vor Ort sind grundsätzlich durch direkte IP-basierte Zugriffsmöglichkeiten aus anderen Zonen und Netzen gefährdet. Dies gilt z. B. aufgrund der besonderen Patch-Zyklen in der OT, die wesentlich länger sein können als z. B. in der Büro-IT. Gleichzeitig erfolgen Fernwartungszugriffe auf ein ICS in der Regel aus nur eingeschränkt vertrauenswürdigen Netzen. Solche Netze sind nicht nur private Netze fremder Institutionen, sondern auch andere Zonen des eigenen Netzes. Nur eingeschränkt vertrauenswürdige

Zonen in der eigenen Institution sind z. B. solche der internen Büro- und Gebäude-IT oder auch weitere Zonen des OT-Netzes (z. B. zur Betriebs- und Produktionsführung mit MES, ERP).

Direktzugriffe aus anderen Zonen und Netzen auf ein ICS, z. B. über eine lokale Verbindung oder über VPN, können Schadprogramme einschleusen und gezielte Angriffe begünstigen. In der Folge können in den zu schützenden OT-Zonen Gefahren für Leib und Leben bestehen, hohe finanzielle Schäden durch Ausfallzeiten drohen oder vertrauliche Informationen wie z. B. Betriebsgeheimnisse in falsche Hände gelangen.

2.6. Unsichere alternative OT-Fernwartungszugänge für Störungen

Insbesondere bei Störungen müssen OT-Fernwartungszugänge zuverlässiger und leistungsfähiger sein als in der Büro- und Gebäude-IT. Im industriellen Umfeld werden daher eigens alternative Fernwartungszugänge für schnelle Zugriffe eingerichtet. Diese stellen die Betriebsfähigkeit des ICS auch dann sicher, wenn der jeweilige primäre Zugang ausfällt oder nicht ausreichend performant ist, um z. B. kritische Fehlerzustände an entfernten Anlagen schnell genug beheben zu können. Solche alternativen Fernwartungszugänge können jedoch besonders verwundbar bei einem Angriff sein.

Wenn ein schneller alternativer Fernwartungszugang, z. B. über Mobilfunk, geschaffen wird, dieser jedoch die Sicherheitsanforderungen der Institution nicht vollständig erfüllt, dann können Angreifende leichter in das OT-Netz eindringen.

2.7. Unsichere Konzeption von OT-Fernwartungszugängen

Häufig besitzt ein ICS eine dezentrale Infrastruktur mit zahlreichen OT-Fernwartungszugängen unterschiedlicher herstellender Unternehmen. Sowohl die unübersichtliche weiträumige Verteilung der Zugänge als auch die vielfältigen proprietären Fernwartungslösungen erschweren eine angemessene zentrale Absicherung sämtlicher OT-Fernwartungszugänge durch die Betreibenden.

Wenn sich OT-Fernwartungszugänge in offen zugänglichen Bereichen befinden, dann können Angreifende über diese Zugänge leicht in OT-Netze eindringen und Manipulationen vornehmen.

Auch wenn OT-Fernwartungszugänge nur durch herstellungsseitig vorgesehene Sicherheitskomponenten geschützt werden und diese die Sicherheitsvorgaben der Institution nicht erfüllen, können Angreifende über diese Zugänge leicht in OT-Netze eindringen und Manipulationen vornehmen.

2.8. Veraltete technische Konzeption von OT-Fernwartungszugängen

Aufgrund der langen Lebenszyklen im industriellen Umfeld gibt es nicht selten OT-Fernwartungslösungen, die zehn Jahre und länger eingesetzt werden und aufgrund ihres Alters Sicherheitslücken aufweisen. Darüber hinaus liegen oft historisch gewachsene spezielle Umgebungsbedingungen vor wie z. B. die Installation von Fernwartungszugängen in offen zugänglichen Bereichen.

Wenn OT-Fernwartungszugänge aufgrund langer Lebenszyklen nicht geeignet abgesichert sind, dann erleichtert dies einen unautorisierten Zugriff in ein ICS und auch in weitere Netze und Systeme innerhalb und außerhalb der OT. So werden Manipulationen möglich, die bis zu Gefährdungen von Leib und Leben führen können.

Darüber hinaus können integrierte Fernwartungszugänge in Anlagen seit vielen Jahren unbekannt sein. Infolge zunehmender Abhängigkeiten von anderen Netzen und Systemen durch jüngere technische Veränderungen können unautorisierte Zugriffe mit kritischen Folgen dann immer wahrscheinlicher werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins IND.3.2 *Fernwartung im industriellen Umfeld* 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	OT-Betrieb
Weitere Zuständigkeiten	IT-Betrieb, Planende, Wartungspersonal, Datenschutzbeauftragte, Mitarbeitende

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.

IND.3.2.A1 Planung des Einsatzes der Fernwartung in der OT (B) [Planende]

Im industriellen Umfeld MUSS für sämtliche Einrichtungen zur Fernwartung ein einheitliches, zentrales Fernwartungskonzept für die gesamte OT der Institution erstellt werden. In dem OT-Fernwartungskonzept MÜSSEN folgende Aspekte berücksichtigt werden:

- spezifische gesetzliche Vorgaben, z. B. Schutz von Personen,
- spezifische Vorgaben durch anlagenherstellende Unternehmen,
- spezifische Anforderungen durch dezentrale Infrastrukturen,
- spezifische Anforderungen an die Anbindungen für die Fernwartung,
- spezifische Anforderungen an die Verfügbarkeit der Fernwartung,
- spezifische Anforderungen durch Umgebungsbedingungen sowie
- spezifische Anforderungen durch Bestandsanlagen.

Alle diese Aspekte MÜSSEN mit sämtlichen beteiligten internen und externen Stellen abgestimmt werden.

Sämtliche Fernwartungszugänge, über die Zugriffe auf ein ICS der Institution möglich sind, MÜSSEN in einer zentralen Dokumentation erfasst werden.

Für neu anzuschaffende fernwartbare Maschinen MÜSSEN die Anforderungen an die Informationssicherheit mit den Liefernden abgestimmt werden.

Das Ziel SOLLTE eine Standardisierung der verwendeten Fernwartungslösungen sein. Sobald standardisierte Lösungen für die Fernwartung geplant werden, MÜSSEN sich die OT und die Büro- und Gebäude-IT gemeinsam abstimmen.

IND.3.2.A2 Konsistente Dokumentation der Fernwartung durch OT sowie Büro- und Gebäude-IT (B) [IT-Betrieb, Wartungspersonal]

Im industriellen Umfeld MÜSSEN die OT und die Büro- und Gebäude-IT sämtliche OT-Fernwartungszugänge gemeinsam erfassen und dokumentieren.

Insbesondere bei Fernwartungskomponenten, die in Package Units integriert sind, MÜSSEN auch alle deaktivierten Zugänge dokumentiert werden.

IND.3.2.A3 Regelmäßige Prüfungen sowie Ausnahmegenehmigungen bestehender OT-Fernwartungszugänge (B) [IT-Betrieb]

Sämtliche Anlagen MÜSSEN regelmäßig geprüft werden, ob alle ihre Fernwartungszugänge dem Soll-Zustand, d. h. dem aktuellen Fernwartungskonzept für die OT, entsprechen.

Für notwendige Abweichungen vom Konzept MUSS innerhalb der OT ein Genehmigungsprozess etabliert werden.

IND.3.2.A4 Verbindliche Regelung der OT-Fernwartung durch Dritte (B)

Mit sämtlichen externen Benutzenden, d. h. herstellenden Unternehmen, Integratoren und Wartungsdienstleistenden, MÜSSEN angemessen restriktive Regelungen für die OT-Fernwartung vertraglich vereinbart werden. Diese vertraglichen Regelungen MÜSSEN zu jedem Zeitpunkt gewährleisten, dass externe Benutzende jegliche OT-Fernwartungszugänge ausschließlich kontrolliert und abgestimmt nutzen.

Intern MUSS festgelegt werden, über welche Fernwartungszugänge welche Tätigkeiten durch welche externen Benutzenden zulässig sind. Darüber hinaus MUSS festgelegt werden, welche internen Mitarbeitende Fernwartungszugriffe und -tätigkeiten von Externen autorisieren, beobachten und gegebenenfalls unterstützen.

Im industriellen Umfeld MUSS sichergestellt werden, dass Personen an oder in Anlagen und Maschinen weder direkt noch indirekt durch eine aktive Fernwartung gefährdet werden können.

Insbesondere bei Safety-Maschinen MUSS der oder die interne OT-Mitarbeitende sowohl organisatorisch als auch technisch die Hoheit über den Beginn und das Ende der Fernwartung haben. Vertraglich MUSS ausgeschlossen werden, dass der Remote-Zugriff ohne explizite Zustimmung der internen OT-Mitarbeitenden aufgebaut und aufrechterhalten werden kann.

IND.3.2.A5 Interne Abstimmung für die OT-Fernwartung mit der Büro- und Gebäude-IT (B) [Planende]

Die OT, die Büro- und Gebäude-IT sowie alle weiteren beteiligten Organisationseinheiten MÜSSEN angemessen restriktive Regelungen für sämtliche Komponenten und Schnittstellen festlegen, die direkt oder indirekt OT-Fernwartung in der Institution ermöglichen. Diese internen Regelungen MÜSSEN zu jedem Zeitpunkt eine kontrollierte und abgestimmte Nutzung der jeweiligen OT-Fernwartungszugänge gewährleisten. Folgende Aspekte MÜSSEN geregelt werden:

- Prozesse
- Zuständigkeiten
- Berechtigungen

IND.3.2.A6 Absicherung jedes Fernwartungszugriffs auf die OT (B) [IT-Betrieb]

Im industriellen Umfeld MUSS die OT jeden Zugriff auf ein IT-System, das einen Fernwartungsdienst für die OT bereitstellt, selbst steuern können. Hierfür MUSS der Zugriff durch mindestens eine Sicherheitskomponente in der Zuständigkeit der OT abgesichert werden.

Der Zugang zur Fernwartung SOLLTE für alle Zugriffe vereinheitlicht werden. Jeder Zugriff SOLLTE mithilfe zentraler Authentisierungskomponenten kontrolliert und explizit zugelassen werden.

Falls Komponenten von OT-Fernwartungszugängen dezentral liegen oder in Package Units integriert sind, dann MÜSSEN diese Zugänge durch eine zusätzliche Sicherheitskomponente abgesichert werden, die ihrerseits zentral liegt und nicht in eine Package Unit integriert ist.

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.

IND.3.2.A7 Technische Entkopplung von Zugriffen (S) [Planende]

Jeder Fernzugriff auf jegliche Komponenten in einer OT-Zone SOLLTE entkoppelt erfolgen. In jedem Fernwartungszugang in die OT SOLLTE ein IT-System positioniert sein, das die Verbindung vor dem Übergang in die OT-Zielzone terminiert und zum Fernwartungsdienst eine neue, überwachte und reglementierte Kommunikation aufbaut.

Alle für die Fernwartung benötigten Werkzeuge und Programme SOLLTEN auf dem IT-System des Fernwartungszugangs installiert und lauffähig sein sowie einen Mehrbenutzendenbetrieb unterstützen. Das IT-System SOLLTE ein Sprungserver oder ein vergleichbares Application Layer Gateway (ALG) sein, das in einem dedizierten Sicherheitssegment, z. B. in einer demilitarisierten Zone (DMZ) positioniert ist.

Für das IT-System zur Entkopplung der Zugriffe SOLLTE die OT zuständig sein, d. h. es liegt idealerweise in einer OT-DMZ.

IND.3.2.A8 Explizite Freigabe jeder OT-Fernwartungssitzung (S) [Mitarbeitende]

Jede Fernwartungssitzung SOLLTE vorab durch einen oder einer OT-Mitarbeitenden der betreibenden Institution, der oder die für das Zielsystem der Sitzung zuständig ist, genehmigt werden. Erst danach SOLLTE der oder die OT-Mitarbeitende den Fernwartungszugang freischalten. Die explizite Freigabe SOLLTE sowohl im Bedarfsfall als auch während abgestimmter Wartungsfenster eingehalten werden. Die Freigabe SOLLTE grundsätzlich nur für einen begrenzten Zeitraum gültig sein, d. h. die zuständigen OT-Mitarbeitenden behalten die Hoheit über den Zeitpunkt der Fernwartung (siehe Anforderung IND.3.2.A3 *Regelmäßige Prüfungen sowie Ausnahmegenehmigungen bestehender OT-Fernwartungszugänge*).

Darüber hinaus SOLLTEN externe Fernwartungszugriffe ausschließlich von innen nach außen, d. h. aus dem OT-Netz heraus, aufgebaut werden.

IND.3.2.A9 Sicherer Austausch von Dateien begleitend zur OT-Fernwartung (S) [Planende, IT-Betrieb]

Für einen Dateiaustausch im Rahmen der OT-Fernwartung, z. B. von Konfigurationsdateien, Updates oder Handbüchern, SOLLTE ein sicheres Vorgehen etabliert werden. Dies MUSS mindestens eine Überprüfung auf Schadsoftware beinhalten.

Der Verbindungsaufbau zwischen einem Datenaustauschsystem und der Dateiquelle SOLLTE nicht automatisiert erfolgen, sondern vor jedem Dateiaustausch von der OT der Institution initiiert und authentisiert werden. Ein Dateiaustausch SOLLTE grundsätzlich protokolliert werden.

IND.3.2.A10 Beobachtung und Kontrolle von OT-Fernwartungssitzungen (S) [Mitarbeitende]

Im industriellen Umfeld MUSS sichergestellt werden, dass weder direkt noch indirekt Personen an oder in Anlagen und Maschinen sowie die Anlagen oder Maschinen selbst durch eine aktive Fernwartung gefährdet werden können. Darüber hinaus MUSS sichergestellt werden, dass eine aktive Fernwartung den Produktionsprozess nicht beeinträchtigt.

Falls Personen- oder Sachschäden möglich sind, MUSS sichergestellt sein, dass die OT-Mitarbeitenden die Fernwartungstätigkeiten vor Ort mitverfolgen können (Vier-Augen-Prinzip). Die OT-Mitarbeitenden SOLLTEN bei Bedarf eingreifen können sowie eine Fernwartungssitzung unterbrechen können.

IND.3.2.A11 Zentrale Verwaltung aller Konten für die OT-Fernwartung (S) [IT-Betrieb]

Für den Fernwartungszugriff in der OT SOLLTEN ausschließlich Konten verwendet werden, die in einem zentralen Verzeichnisdienst der OT oder der Institution verwaltet werden.

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.

IND.3.2.A12 Dedizierte Fernwartungslösung in der OT (H) [Planende]

Für die Fernwartung im industriellen Umfeld SOLLTE eine dedizierte OT-Fernwartungslösung eingesetzt werden, die unabhängig von der Büro- und Gebäude-IT ist. Alle weiteren Funktionen auf den IT-Systemen zur OT-Fernwartung, insbesondere auch Funktionen zur Administration von IT-Systemen und Netzen außerhalb der OT, SOLLTEN deaktiviert bzw. unterbunden werden.

Falls eine maximale Unabhängigkeit realisiert werden soll, SOLLTE auch ein dedizierter Internet-Zugang für die OT-Fernwartung genutzt werden.

IND.3.2.A13 Protokollierung der Inhalte von Fernwartungszugriffen in der OT (H) [Planende, Datenschutzbeauftragte]

Für die Fernwartung von OT-Anwendungen oder -Systemen SOLLTE die Protokollierung so ausgeweitet werden, dass sämtliche Tätigkeiten lückenlos und umgehend nachvollziehbar sind. Hierzu SOLLTEN ergänzend zur Protokollierung von Ereignissen und Sitzungsdaten auch die Inhalte von Fernwartungszugriffen protokolliert werden.

IND.3.2.A14 Technische Kontrolle von Fernwartungssitzungen (H) [Planende, Datenschutzbeauftragte]

OT-Fernwartungssitzungen SOLLTEN ergänzend zu IND.3.2.A10 *Beobachtung und Kontrolle von OT-Fernwartungssitzungen* kontinuierlich durch eine technische Lösung reglementiert werden. Dabei SOLLTEN die Aktivitäten auf Befehlsebene, d. h. manuelle und automatisierte Befehle, technisch überwacht und gegebenenfalls automatisch unterbunden werden.

Zusätzlich SOLLTEN Sitzungen komponentenübergreifend überwacht werden. Falls technisch überwacht wird, dann SOLLTE nicht nur bei konkreten Regelverstößen, sondern auch bei Anomalien im Benutzungsverhalten ein Alarm ausgelöst werden, z. B. sobald ein plötzlich erhöhtes Kommunikationsvolumen erkannt wird.

4. Weiterführende Informationen

4.1. Wissenswertes

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

Das Bundesamt für Sicherheit in der Informationstechnik beschreibt in seiner Veröffentlichung „ICS Security Kompendium" die Absicherung von industriellen Systemen (ICS, Industrial Control Systems).