Inhaltsverzeichnis

1 Allgemeines

Hat der Auftragnehmer (AN) für den Auftraggeber (AG) IT-/OT-Systeme zu liefern, zu entwickeln und/oder instand zu halten, gilt dieses Dokument ergänzend zu einer ggf. vorliegenden Spezifikation - wie bspw. einer Technischen Spezifikation oder funktionalen Aufgabenbeschreibung oder funktionalen Aufgabenstellung eines Leittechnik- oder IT-Projekts - des AG. Der AN hat die Anforderungen dieses Dokumentes bereits bei seiner Angebotserstellung und Angebotsabgabe zu berücksichtigen.

IT-/OT-Systeme sind vom AN gemäß dem allgemein anerkannten Stand der Technik und den geltenden Standards der Informationssicherheit sowie den gültigen Gesetzen und untergesetzlichen Regelwerken, wie bspw. ISO/IEC 27002, ISO/IEC 27019 und BDEW-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ jeweils in der gültigen Fassung einzurichten.

Erkennt der AN, dass über die darin beschriebenen Anforderungen hinaus noch weitere Anforderungen zu erfüllen sind, so ist er verpflichtet, dies dem AG mitzuteilen.

Hinsichtlich der Sicherstellung der Informationssicherheit des vom AN geschuldeten Liefer- und Leistungsumfangs hat der AN ein Informationssicherheitskonzept gemäß ISO/IEC 27001 kostenfrei zu erstellen. Die Umsetzung des abgestimmten Informationssicherheitskonzeptes weist der AN dem AG nach. Bei Tätigkeiten an Standorten des AG (einschließlich des Fernzugriffs auf die IT-/OT-Infrastruktur des AG) sind durch den AN zusätzlich das Merkblatt des AG „Merkblatt für unternehmensfremde Personen zur Gewährleistung der Sicherheit in der Informationstechnik (Informationssicherheit) von MIBRAG“ zu beachten.

2 Umzusetzende Maßnahmen

2.1 Benutzerverwaltung

In den IT-/OT-Systemen ist für jeden Benutzer ein eigenes Benutzerkonto einzurichten. Dies gilt sowohl für die Betriebssystemebene (z. B. Windows) als auch für die Anwendungsebene (z. B. Win CC).

Für Benutzer mit gleichartigen Aufgaben (z. B die Gruppe der Leitstandfahrer bzw. die Gruppe der Techniker) sind einheitliche Benutzerrollen zu definieren, die entsprechend ihrem Tätigkeitsfeld die notwendigen Rechte erhalten. Bei der Erstellung von Benutzerrollen sind nur solche Rechte zu vergeben, die für die Erfüllung der jeweiligen Aufgabe notwendig sind (Need-To-Know-Prinzip).

Jeder Benutzer hat sich bei Aufnahme seiner Tätigkeit mit seinen persönlichen Zugangsdaten am jeweiligen System anzumelden. Der Zugriff auf die Systeme ist personenscharf zu registrieren.

Eine Anmeldung als Benutzergruppe (z. B. eine einmalige und dauerhafte Anmeldung als Gruppe Leitstandfahrer) ist nicht zulässig. Sofern aus technischen Gründen eine Anmeldung als Benutzergruppe notwendig ist, ist eine Ausnahmeregelung zu definieren und durch den Informationssicherheitsbeauftragten des AG freizugeben.

Die Zugehörigkeit des AG-Personals zu den jeweiligen Benutzerrollen wird vom AG vorgegeben.

Die Realisierung der Zugriffskontrolle und Benutzerverwaltung hat bei umfangreichen Anlagen durch Domänencontroller zu erfolgen. Dabei sind notwendige Redundanzen zu berücksichtigen. Auf kleineren Anlagen können auch alternative Verfahren eingesetzt werden. Das zum Einsatz kommende Verfahren, inklusive der erstellten Rollen und deren Beschreibungen ist mit dem AG abzustimmen und durch den AN zu dokumentieren.

2.2 Standardpasswörter

Alle Standardpasswörter der Hersteller sind bis zur Inbetriebnahme von den Systemen zu entfernen und durch individuelle Passwörter zu ersetzen. Dazu zählen auch Passwörter auf eventuellen Netzwerk- und anderen Peripheriekomponenten.

Systeme müssen eine Passwortrichtlinie gemäß dem aktuellen Stand der Technik unterstützen, die jeweilige Anforderung (Komplexität) an die Passwörter sind mit dem AG abzustimmen. Passwörter und andere Authentisierungsinformationen dürfen nur verschlüsselt übertragen und im System gespeichert werden.

Auf prozessnahen Komponenten wie speicherprogrammierbaren Steuerungen (SPS) und Automatisierungskomponenten oder Gateways sind vorhandene Standardpasswörter auf sichere Werte zu setzen sowie sicherheitserhöhende Konfigurationsoptionen zu aktivieren.

Für Systeme zur Remoteanbindung ist eine 2-Faktor-Authentifizierung umzusetzen.

Im Falle einer Störung des Benutzerverwaltungsdienstes sind lokale Notfallpasswörter vorzusehen.

2.3 Protokollierung

Systeme und Komponenten sind so zu planen, dass An- und Abmeldevorgänge der Benutzer sowie weitere Systemereignisse automatisch protokolliert und zentral gespeichert werden. Weitere Kriterien wie z. B. Zeitraum und Anzahl der zu speichernden Meldungen sind mit dem AG abzustimmen. Mit dem AN ist abzustimmen, wie und wo die jeweiligen Protokolle für eine regelmäßige Routinekontrolle einzusehen sind.

Die Protokollierung muss sowohl für die Betriebssystemebene (Windows) als auch die Anwendungsebene erfolgen. Alle Systeme sind auf eine einheitliche Systemzeit zu synchronisieren.

Prozessnahe Komponenten wie speicherprogrammierbare Steuerungen (SPS) und Automatisierungskomponenten sind so zu planen, dass Systemereignisse und Protokolle erstellt und an einen zentralen Speicher zur Auswertung übertragen werden.

2.4 Sicherheits-Patches

Sämtliche in den IT-/OT-Systemen eingesetzte Komponenten sind mit aktuellen und vom Hersteller geprüften und zugelassenen Sicherheits-Patches zu versehen. Die jeweils aktuell verwendeten Sicherheits-Patches sind in geeigneter Weise zu dokumentieren. Zum Abschluss der örtlichen Bau-/Inbetriebnahme-Phase müssen die vom jeweiligen Hersteller aktuell freigegebenen Sicherheits-Patche auf den Systemen installiert sein.

Zwischen AG und AN ist ein geeignetes Verfahren zur Aktualisierung der Sicherheits-Patches für die Betriebszeit nach der Inbetriebnahme (Gewährleistungszeit) abzustimmen. Hierzu zählen auch eventuelle Fallback- bzw. Rollbackfunktionen für den Fall von fehlerhaften Sicherheits-Patches. Ggf. ist hierzu ein Wartungsvertrag mit dem AG abzuschließen.

2.5 Softwarestände und Lizenzen

Die aktuell verwendeten Softwarestände und Lizenzen sind in geeigneter Weise und nach den Vorgaben des ISMS des AG zu dokumentieren und sicher zu archivieren. Es darf nur Software eingesetzt werden, die vom Hersteller für die jeweiligen Systeme freigegeben ist.

2.6 Einsatz von Virenscannern

Alle vernetzten Komponenten, welche in den IT-/OT-Systemen zum Einsatz kommen, sind an geeigneter Stelle mit vom jeweiligen Hersteller zugelassenen Virenscannern auszurüsten. Die Virenscanner sind in der vom Hersteller vorgegebenen Weise zu konfigurieren. Sofern die

technische Entwicklung der Hersteller eine kontinuierliche und rückwirkungsfreie Virenüberwachung zulässt, ist diese zu realisieren. Die notwendigen Reaktionszeiten des jeweiligen OT-Systems dürfen jedoch nicht negativ beeinflusst werden. Andernfalls sollte der Scanvorgang nicht kontinuierlich erfolgen, sondern kann in festzulegenden Zyklen oder auf Anforderung erfolgen (z. B. 1x täglich oder wöchentlich usw.).

Das vorgesehene Verfahren zur Aktualisierung der Virensignaturen ist zu beschreiben. Neue Virenpattern sind über eine Datenschleuse in eine dafür vorgesehenen Demilitarisierten Zone (DMZ) einzuspielen. Der aktuell verwendete Stand der Virensignaturen ist in geeigneter Weise zu dokumentieren.

2.7 Unbelegte USB-Zugänge der OT-Systeme

Unbelegte USB-Zugänge außerhalb der verschlossenen Serverschränke sind zu deaktivieren. Wo das Deaktivieren aus betrieblicher Sicht nicht möglich oder sinnvoll ist, sind mechanische USB-Schlösser vorzusehen.

2.8 Verschlossenen Systemschränke der OT-Systeme

Die Server- und Automationsschränke (inkl. möglicher Seitenwände) sind mit eigener Schließung zu versehen. Die Schließung darf nicht mit einer Standard-Schließung für Serverschränke erfolgen und ist mit dem AG im Vorfeld abzustimmen.

2.9 Netzwerkzugänge

Alle Netzwerkzugänge innerhalb der IT-/OT-Systeme sind gem. Abschnitt 2.1.3 zu überwachen und eventuelle Systemereignisse zu protokollieren. Es ist ein Verfahren zu integrieren, das nur bekannte Teilnehmer im Netzwerk akzeptiert. Unbekannte Teilnehmer (wie z. B. nachträglich in freie Netzwerkzugänge eingesteckte Laptops) sind von den OT-Systemen abzuweisen.

Es ist sicherzustellen, dass kein unzulässiger Zugriff auf die OT-Systeme, z. B. durch eine am Drucker abgezogene Netzwerkleitung, erfolgen kann.

Unbelegte Netzwerkzugänge außerhalb von verschlossenen Serverschränken, wie z. B. an Switches im Feld, sind zu deaktivieren oder mechanisch zu verschließen.

2.10 Verbindung der OT-Systeme mit externen Netzen

Für einen eventuellen Datenaustausch mit zentral bereitgestellten MIBRAG-Diensten sind die OT-Systeme an zentraler Stelle mit dem MIBRAG IT-Netzwerk verbunden. Hierzu ist zwischen den OT-Systemen und dem IT-Netzwerk (Büro-Netzwerk) eine DMZ mit Datenschnittstelle vorzusehen bzw. in Abstimmung mit dem AG eine bestehende DMZ zu nutzen.

2.11 Firewalls zu externen Systemen

Sämtliche Schnittstellen von IT-/OT-Systemen zu Systemen Dritter (externer oder fremder Partner) sind durch Firewalls mit restriktivem Regelsatz zu sichern und die Kommunikation der OT-Systeme darf nur über eine DMZ erfolgen. Sofern im begründeten Ausnahmefall das OT-System direkt mit Systemen Dritter kommunizieren muss, darf dies nur über vom AG zugelassene Verbindungen (Site2Site VPN) mit entsprechenden Firewalls und Sicherheitsmechanismen erfolgen.

Jeder Einzelfall ist vom AG ausdrücklich freizugeben und im Detail mit ihm abzustimmen.

Die Firewall-Regeln werden vom AG vorgegeben und sind in den vom AN zu liefernden Komponenten der IT-/OT-Systeme zu berücksichtigen. Technische Details sind projektspezifisch mit dem AG abzustimmen.

2.12 Sicherer Fernzugang

Zur Systemunterstützung während der Bau- und der späteren Betriebsphase besteht die Möglichkeit dem AN einen Fernzugang für den Zugriff auf die OT-Systeme über öffentliche Netze einzurichten.

Die Authentifizierung der Benutzer hat ausschließlich über Zwei-Faktor-Authentifizierung zu erfolgen.

Darüber hinaus und sofern die Bereitstellung einer Architektur für Fernzugriffe Bestandteil der Beauftragung ist, gelten folgende Vorgaben und Anforderungen:

Die Datenübertragung über das Internet oder Internet-ähnliche Netze zwischen Client und Remote Access-Gateway muss stark verschlüsselt erfolgen und über Site2Site VPN realisiert werden.

Die Architektur der Fernzugänge muss eine Isolation des Prozessnetzes sicherstellen und eine direkte Einwahl in die Endgeräte der Prozessleittechnik unterbinden. Um dies sicherzustellen, muss ein Fernzugriff über eine DMZ und einen zentral verwalteten Zugangsserver (Remote Access-Gateway, Terminalserver, JumpHost) des AG erfolgen. Beim Verbindungsaufbau hat der AN dafür Sorge zu tragen, dass der Virenschutz und Patchstand der Endgeräte aktuell ist.

Der Zugriff auf einen Fernzugang muss zentral geloggt und wiederholte Fehlversuche gemeldet werden. Alle Fern-Zugangs-Möglichkeiten sind zu dokumentieren und individuell durch eine berechtigte Person des AG freizugeben. Handlungstätigkeiten sind zu überwachen, evtl. Systeme zur Aufzeichnung dieser Tätigkeiten sind entsprechend zu planen. Es ist zudem eine automatische Sperrung des Fernzugang nach den Vorgaben des AG umzusetzen.

Sofern der AN Leistungen zur Systemunterstützung über einen Fernzugang erbringt, sind entsprechende Vertraulichkeitsvereinbarungen zwischen AN und AG zu vereinbaren.

2.13 Datenschleuse zum sicheren Datenaustausch mit den OT-Systemen

Um einen sicheren Datenaustausch mit externen Netzen (z. B. Büro-IT, Fernwartung etc.) zu gewährleisten, ist innerhalb der DMZ eine Datenschleuse bzw. Datengateway einzurichten.

Das Einlesen bzw. das Auslesen von Daten in das bzw. aus dem OT-System, darf grundsätzlich nur über diese vom AG kontrollierte Datenschleuse und über sichere Protokollvarianten (z. B. sFTP) erfolgen. Der direkte Datenaustausch über USB-Sticks oder ähnliches ist nicht gestattet.

Details zum Umgang mit der Datenschleuse werden dem AN nach Auftragserteilung mitgeteilt. Sofern die Bereitstellung einer Datenschleuse Bestandteil der Beauftragung ist, gelten insbesondere die in diesem Dokument definierten Vorgaben zur Benutzerverwaltung, Passwortnutzung, Sicherheitspatches und Kryptografie als Mindestanforderungen. Weitere Details zur Bereitstellung einer Datenschleuse sind mit dem AG abzustimmen.

2.14 Kryptografie

Grundsätzlich soll die Kommunikation der IT-/OT-Systeme untereinander, sowie auch die Kommunikation mit externen Systemen, durch kryptographische Verfahren gesichert werden. Passwörter dürfen grundsätzlich nicht im Klartext übertragen oder bei der Eingabe auf dem Bildschirm sichtbar werden. Es dürfen nur Verschlüsselungsverfahren verwendet werden, deren Sicherheit nach dem Stand der Technik als ausreichend für den jeweiligen Einsatz und die jeweilige Einsatzdauer bewertet sind. Die Auswahl der zu verwendenden Verschlüsselungs-verfahren erfolgt durch Abstimmung mit dem AG auf Grundlage des Dokumentes vom Bundesamt für Sicherheit in der Informationstechnik (BSI) „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ in der jeweils aktuellen Version. Darüber hinaus definiert die IEC-62351 den aktuellen Stand der Technik und die Anforderungen an die Verschlüsselung für Prozess-steuerungssysteme. Weitere Details sind der Sicherheits- und Schutzsystemleitlinie ISMS – Kryptographie des AG zu entnehmen.

Wenn die Gefahr besteht, dass Laufzeiten und Reaktionszeiten von OT-Systemen durch kryptographische Verfahren negativ beeinflusst werden, kann bei interner Kommunikation der OT-Systeme auf kryptographische Verfahren verzichtet werden. In diesem Fall sind weitergehende Sicherheitsmaßnahmen (z. B. IDS, Application Whitelisting etc.) mit dem AG abzustimmen.

Der AN erstellt grundsätzlich einen Übersichtsplan seines Liefer- und Leistungsumfangs, in dem der Einsatz kryptografischer Verfahren erkennbar ist. Sämtliche zur Anwendung kommenden Lösungen sind mit dem AG abzustimmen.

2.15 IDS (Intrusion Detection System) und OT-Monitoring System

Ein Intrusion Detection System bzw. eine Funktion zur Überwachung des Datenverkehrs im OT-System (OT-Monitoring) ist zu integrieren. Sofern die Bereitstellung eines solchen Systems Bestandteil der Beauftragung ist, muss im Vorfeld eine enge Abstimmung mit dem AG bezüglich der Auswahl eines solchen Systems erfolgen. Folgende Funktionen sind durch ein solches System mindestens bereitzustellen:

- Automatische Erkennung und Inventarisierung von sämtlichen OT- und Netzwerkkomponenten
- Erstellung und Überwachung einer sog. Baseline und Alarmierung bei Verletzung dieser
- Erkennung und Überwachung von Parameter-, Funktions- und Konfigurationsänderungen
- Schwachstellen-Management anhand von Signaturen, Anomalien und bekannten Schwachstellen
- Heuristische Scans zur Erkennung von akuten Cyberangriffen (z. B. Man-in-the-middle-Angriff, Port-Scan)
- Überwachung und Erkennen von eventuellen weiteren Bedrohungen (z. B. häufige fehlschlagende Anmeldeversuche)
- Sichere Fernzugänge, sofern nicht durch andere Systeme bereits vorhanden.

Netzwerkgeräte und prozessnahe Komponenten wie Steuerungen, speicherprogrammierbare Steuerungen (SPS) und Automatisierungskomponenten sind möglichst dahingehend auszuwählen, dass eine Funktion zur Überwachung (z. B. SPAN, Mirror-Port) durch den Hersteller bereits integriert ist. Die Auswahl eines Herstellers solcher Komponenten ist grundsätzlich mit dem AG abzustimmen.

2.16 Backupverfahren

Vor und nach jeder Änderung der Anwendersoftware, der Firmware und des Betriebssystems, ist grundsätzlich ein Backup zu erstellen. Die Backups sind auf NAS-Laufwerken oder auf zentralen Bereichsservern redundant in verschiedenen Brandabschnitten abzulegen. Alternativ können virengeprüfte und vom AG freigegebene mobile Datenträger genutzt werden. Alle Backups sind eindeutig zu kennzeichnen und an einem sicheren Ort aufzubewahren.

Es sind Mechanismen zu planen, mit denen die Vollständigkeit und Korrektheit einer Datensicherung gegen den aktuellen Datenbestand geprüft werden kann. Die Datensicherungs- und Rücksicherungsverfahren sind ausführlich zu dokumentieren.

Das zur Anwendung kommende Verfahren ist mit dem AG abzustimmen.

2.17 Umgang mit nicht mehr genutzten Datenträgern und Datenaufzeichnungen

Alle nicht mehr genutzten Datenträger oder Aufzeichnungen von Daten/Informationen sind sicher und vertraulich zu vernichten und deren Vernichtung ist zu dokumentieren. Dazu sind diese dem AG zu übergeben oder nachweisbar entsprechend den Vorgaben des AG zu entsorgen.

2.18 Umgang mit Service-Laptops in OT-Systemen

Zur Parametrierung oder ähnlichen Tätigkeiten sind vorzugweise Service-Laptops des AG zu nutzen. Die Nutzungsbedingungen und Vereinbarungen sind durch den AG entsprechend zu kommunizieren und dokumentieren.

Sofern Service-Laptops oder PCs des AN genutzt werden müssen und mit dem OT-System des AG verbunden werden, ist durch den AN vor Ort die Virenfreiheit dieser Geräte zu prüfen und nachzuweisen. Der Vorgang ist entsprechend zu dokumentieren.

2.19 Asset-Management

Zur Integration in das ISMS (Informations-Sicherheits-Management-System) des AG sind alle zum Lieferumfang gehörenden Hard- und Softwarekomponenten durch den AN in einer Asset-Liste nach den Vorgaben des AG zu erfassen und dem AG bereitzustellen.

2.20 Dokumentation

Alle im Rahmen der Systemhärtung erbrachten Lieferungen und Leistungen sind im Rahmen dokumentierter Bedienabläufe nach DIN ISO/IEC 27001 durch den AN zu beschrieben, hierzu stellt der AG ein entsprechendes Template zur Verfügung. Die Dokumentation ist durch den AG abzunehmen.

2.21 IT-/OT-Systeme – Prüfung, Abnahme und Dokumentation

Die Erfüllung aller in diesem Dokument beschriebenen Anforderungen ist im Rahmen der Werkfunktionsprüfung bzw. spätestens zur Abnahme auf der Baustelle vom AN nachzuweisen und in einer Checkliste zu dokumentieren. Die Inhalte der Checkliste sind im Vorfeld mit dem AG abzustimmen.

Zum Ende der Bauphase und bei der Inbetriebnahme vor Ort und vor Verlassen der Baustelle hat der AN noch einmal die Virenfreiheit der Systeme nachzuweisen und zu dokumentieren.

Im Rahmen der Abnahme wird die Einhaltung der Mindestanforderungen der Informationssicherheit vom AG überprüft und im Abnahmeprotokoll dokumentiert.

3 Umgang mit Informationssicherheitsvorfällen

Mögliche Informationssicherheitsvorfälle, die Auswirkung auf Informationswerte oder Prozesse des AG haben können, sind dem AG unverzüglich mitzuteilen. Hierzu unterweist der AN alle Mitarbeiter dahingehend, dass sie:

- in der Lage sind, Informationssicherheitsvorfälle zuverlässig zu erkennen,
- die sie betreffenden Meldewege für Informationssicherheitsvorfälle kennen, und
- sich ihrer Verpflichtung zur umgehenden Meldung bewusst sind.

Der AN etabliert die erforderlichen internen Prozesse, um eine unverzügliche Meldung an den AG zu gewährleisten.

Die Meldung erfolgt an den jeweiligen fachlichen Ansprechpartner des AG, bei erkennbarer Dringlichkeit auch **zusätzlich** direkt per E-Mail an: informationssicherheit@mibrag.de