

Anlage D: Service Guide

Das nachfolgend aufgelistete Service-Portfolio wird regelmäßig an den Kundenbedarf angepasst und weiterentwickelt.

Für nicht im Service Guide aufgeführte Leistungen bedarf es der Klärung zwischen dem Kunden und der abwickelnden Serviceeinheit von ProLeiT/Schneider Electric.

1 Definitionen

1.1 ITIL

Bei der Erbringung der Serviceleistungen orientiert sich ProLeiT an ITIL (IT Infrastructure Library), den weltweiten Best Practices für IT-Service-Management.

1.2 Service Request

Ein Service Request ist die Anfrage eines Kunden, welche nicht die Behebung von Störungen erfordert. Der Service Request definiert eine formale Kundenanfrage zur Bereitstellung von Informationen oder Unterstützung sowie Beratungsleistungen (Consulting).

Beispiele in Bezug auf Automatisierungssysteme und Manufacturing Execution Systems (MES):

- Bereitstellen von Patches und / oder Installationsmedien
- Projektierungsunterstützung
- Beratung zu den Softwarekomponenten
- Standard-Changes (Passwortänderungen u.ä.)
- Informationsanfragen (Handbucharforderungen, Beratungswünsche, o. ä.)
- Erstellung von Reports

1.3 Incident

Ein Incident (Störung) definiert eine ungeplante Unterbrechung eines IT-Services oder eine Qualitätsminderung eines IT-Services.

Beispiele in Bezug auf Automatisierungssysteme und Manufacturing Execution Systems (MES):

- Ausfall / Störung der Kommunikation zwischen Server und SPS (PLS)
- Ausfall von Hardwarekomponenten
- Lange Antwortzeiten bei der Anlagenbedienung

Die Einordnung der Incidents (Störungen) erfolgt durch ProLeiT unter angemessener Berücksichtigung der Dringlichkeit und der Auswirkungen der gemeldeten Fehler oder Störungen auf den Geschäftsbetrieb des Kunden. Es gilt folgende Matrix:

Dringlichkeit	Auswirkung		
	hoch	mittel	niedrig
hoch	Prio 1	Prio 2	Prio 3
mittel	Prio 2	Prio 3	Prio 4
niedrig	Prio 3	Prio 4	Prio 4

Dringlichkeit: Maß für die Schnelligkeit, mit der eine Störung behoben werden muss

Auswirkung: Ausmaß einer Störung: Wer oder was ist in welchem Umfang betroffen?

Im Rahmen dieser Servicevereinbarung unterscheidet ProLeiT die Incidents in:

- „Major Incident“ = Incident der Priorität 1 oder 2
Ein „Major Incident“ ist eine Störung, die den Ausfall wesentlicher Systembestandteile oder des Gesamtsystems verursacht, so dass die Nutzung vollständig verhindert wird und eine sofortige Störungsbeseitigung unumgänglich ist.
Ein nicht produktives System (z. B. Testsystem) kann keinen „Major Incident“ auslösen.
Beispiele:
 - Prio 1: Anlagenstillstand, es kann nicht weiter produziert werden.
 - Prio 2: Produktion ist erheblich beeinträchtigt oder Produktionsstillstand droht.
- „Minor Incident“ = Incident der Priorität 3 oder 4
Ein „Minor Incident“ ist eine mittelbare Beeinträchtigung der Produktion oder ein Fehler bzw. eine Störung ohne Beeinträchtigung der Produktion.
 - Prio 3: Mittelbare Beeinträchtigung der Produktion
 - Prio 4: Es erscheint eine Fehlermeldung, nach deren Bestätigung kann aber normal weitergearbeitet werden.

1.4 Event

Ein Event (Ereignis) ist eine Statusänderung sowie ein Alarm oder eine Benachrichtigung, die durch das Event Management erzeugt wurde.

1.5 Problem

Ein Problem ist die Ursache für einen oder mehrere Incidents. Mittels eines Problem-Tickets werden die Ursachen von Störungen analysiert und Maßnahmen zu ihrer Verhinderung oder Behebung entwickelt.

1.6 Change

Der Change (Änderung) definiert ein Hinzufügen, Ändern oder Entfernen von Hardware- oder Softwarekomponenten oder Teilen davon.

Beispiele in Bezug auf Automatisierungssysteme und Manufacturing Execution Systems (MES):

- Austausch der Hardware
- Installation neuer Softwarekomponenten oder Softwareupdates oder sonstiger Patches
- Änderungen der Projektierung

Generell wird zwischen ‚Normal Change‘, ‚Standard Change‘ und ‚Emergency Change‘ unterschieden:

- **Normal Change**
Normal Changes sind z.B. Erweiterungen, Änderungen oder Optimierungen der Projektierung, Installation von Patches des Betriebssystems, des SQL Servers oder Drittsoftware, die auch ProLeiT Software betreffen.
Jeder Normal Change durchläuft den üblichen Freigabeprozess.
- **Standard Change**
Standard Changes sind Änderungen, für die in der Regel genaue Verfahrensanweisungen existieren: Da mit ihnen nur niedriges Risiko einhergeht, benötigen sie keine (weiteren) Freigabeprozesse.
Die Priorisierung der Changes ergibt sich aus der Betrachtung von Auswirkung und Dringlichkeit. Bei hoher Auswirkung und hoher Dringlichkeit ergibt sich auch eine hohe Priorität des Request for Change (RfC) und umgekehrt.
- **Emergency Change**
Der Emergency Change durchläuft nicht den üblichen Prozess, sondern wird sofort, notfalls auch

unter erheblichem Risiko und ohne weitere Genehmigung, meist zur Abwendung größeren Schadens durchgeführt.

1.7 Patch

Ein Patch ist eine Korrekturauslieferung für Software oder Daten aus Endanwendersicht, um Fehler zu beheben – meist um bekannt gewordene Sicherheitslücken zu schließen – oder bislang nicht vorhandene Funktionen nachzurüsten. Es ist zwischen brewmaxx / Plant iT Patches und 3rd Party Patches zu unterscheiden.

1.8 Servicezeit

Die Servicezeit beschreibt die Zeitspanne, in der die angebotenen Leistungen von ProLeiT erbracht werden. Die Servicezeit richtet sich nach dem gewählten Vertragsmodell.

1.9 Geschäftszeit

Es gilt die Geschäftszeit von ProLeiT am Standort Herzogenaurach (Bayern, Deutschland).

Geschäftszeit ist werktags von **Montag bis Freitag zwischen 9:00 und 17:00 Uhr (MEZ)** ausschließlich der gesetzlichen Feiertage sowie samstags und sonntags.

Eine andere Regelung (z.B. Geschäftszeit einer Tochtergesellschaft an einem anderen Standort) muss in der **Anlage A** – Kapitel 7 beschrieben werden.

1.10 Reaktionszeit

Die Reaktionszeit ist die Zeitspanne vom Eingang und der Erfassung eines Incidents bis zum ersten Kontakt durch ProLeiT mit dem Kunden. Die Reaktion kann telefonisch oder per E-Mail erfolgen.

Die Reaktionszeiten gelten ausschließlich für Systeme im produktiven Einsatz.

Die Erstreaktion durch ProLeiT auf Major Incidents erfolgt immer telefonisch.

Die Störungsmeldung außerhalb der Geschäftszeit muss telefonisch mit dem Hinweis erfolgen, dass eine Bearbeitung als Major Incident gewünscht wird. Außerhalb der Geschäftszeit wird ProLeiT ausschließlich Major Incidents bearbeiten. ProLeiT beurteilt und bearbeitet diese Störung entsprechend den Kapiteln 1.2 Service Request und 1.3 Incident, den gewählten Services aus **Anlage A** und den entsprechenden Reaktionszeiten aus **Anlage C**.

Die Reaktionszeiten richten sich nach dem gewählten Servicemodell.

1.11 Serviceerbringungspunkt

Der Serviceerbringungspunkt ist der physische Standort, von dem aus der Service erbracht wird.

Die Kontaktdaten werden nach Vertragsschluss über ein SLA Zertifikat mitgeteilt, in dem alle benötigten Informationen des Servicevertrags enthalten sind.

1.12 Korrespondenzsprache

Sämtliche Kommunikation, schriftlich wie mündlich, erfolgt in deutscher oder englischer Sprache. Abweichende Regelungen müssen vertraglich vereinbart werden, siehe **Anlage A** – Kapitel 7.

Die Dokumentation im Ticketsystem sowie der Health Check Report (siehe Kapitel 2.4.2.1 Remote Health Check und Kapitel 2.4.2.2 On-Site Health Check) werden ausschließlich in Deutsch oder Englisch verfasst.

2 Serviceleistungen

2.1 Anfragen-Management

ProLeiT hält qualifiziertes Servicepersonal für die Erbringung der beschriebenen Leistungen vor. Kundenanfragen werden per Telefon oder E-Mail an den zentralen Helpdesk in Herzogenaurach oder den in der **Anlage A** – Kapitel 7 vereinbarten Serviceerbringungspunkt übermittelt und im Ticketsystem der ProLeiT erfasst. Nach der Kategorisierung und Priorisierung (siehe Kapitel 1.2– Kapitel 1.6) erfolgt die weitere Bearbeitung gemäß der ProLeiT-Prozesse für:

- Incident Management
- Service Request Management und
- Escalation Management

Hierfür setzt ProLeiT auf eine Remote Einwahl zum Kundensystem (siehe Kapitel 2.4.1). Zusätzlich betreibt ProLeiT Systemumgebungen der passenden Version von Plant iT / brewmaxx zur Fehleranalyse.

Das System Monitoring (siehe Kapitel 2.4.2.3) unterstützt bei der Ermittlung von Störungsursachen.

2.1.1 Incident Management

Beseitigung ungeplant auftretender Störungen (Incident) durch Herstellerexpertise mittels:

- Vorgehen nach an ITIL angelehntem Standardprozess
- Fehleranalyse inklusive Unterstützung bei der Wiederherstellung der Betriebsbereitschaft ausgelöst durch Störungen oder den Ausfall von Komponenten des PLS/MES gemäß Anlage A
- Sammlung von Diagnosedaten zur Eingrenzung der Fehlerursache
- Unterstützung bei der Fehlerbehebung oder Umgehung des Fehlers durch einen Workaround
- Ticketdokumentation inklusive vorgenommener Änderungen an der Konfiguration / Installation
- Mitteilung des Bearbeitungsstatus
- Überführung in Changes / Problems, wenn erforderlich
- Bereitstellung von Patches und Updates zur Fehlerbehebung für die vertraglich festgelegten Computerprogramme (ProLeiT Systemsoftware) gemäß Anlage A.
- Sollte eine Störungsbeseitigung per Remote Einwahl nicht möglich sein, kann ein Vor-Ort-Support nach Rücksprache mit ProLeiT vereinbart werden. Liegt eine Reisewarnung des Auswärtigen Amtes der Bundesrepublik Deutschland vor, ist ProLeiT nicht zur Durchführung eines Vor-Ort-Support verpflichtet. Die genauen Bestimmungen für einen Vor-Ort-Support werden in Anlage A– Kapitel 7 vereinbart.

2.1.2 Escalation Management

ProLeiT bietet in Abstimmung mit dem Kunden ein prioritätengestaffelt Eskalationsmanagement. Je nach Kategorisierung des Incidents wird die Unterstützung durch Experten sichergestellt. Beispiele für Eskalationen sind:

- Application Support: Weitere Unterstützung durch Projektteam
- Product Support: Eskalation an die Abteilungsleitung des Supports
- IT Support: ProLeiT IT-Abteilung oder Hersteller

2.1.3 Service Request Management

Beantwortung der Kundenanfrage durch

- Consulting-Leistungen (Service Request)
- Bearbeiten von Serviceanfragen (Service Request, Change)

- Beratung und Auskunftserteilung per Telefon zu allen Funktionen der ProLeiT Software
- Unterstützung bei der Anpassung von Hard- und Softwarekonfigurationen durch qualifiziertes Personal mit Erfahrung in der Projektierung von ProLeiT Software sowie Anlagenerfahrung per Telefon / Remote Access
- Optimierungen z. B. zusätzliche Meldetexte und Abfragen
- Mitteilung des Bearbeitungsstatus
- Überführung in Changes / Problems, wenn erforderlich

2.1.4 Self-Service-Portal

Jeder SLA-Kunde erhält Webzugriff auf das mySchneider Portal. Damit werden unter anderem folgende Funktionen bereitgestellt:

- Erstellen von Tickets und Ergänzung von Hinweisen, Kommentaren und Rückfragen zum Ticket
- Gesamtüberblick über alle Tickets des eigenen Unternehmens und somit Vermeidung von Doppelanfragen zu ein und demselben Thema
- Einsicht des Ticketstatus
- Übersicht der Credit-Buchungen
- Dokumentation aller erbrachten Serviceleistungen
- Mit dem Self-Service-Portal hat der Kunde Transparenz über die geleisteten Services.

2.2 Product Support

ProLeiT bietet Product Support für die Softwareprodukte Plant iT und brewmaxx sowie deren Add-Ons und Module.

Die Bearbeitung der Kundenanfrage erfolgt gemäß Kapitel 2.1 und wird vom zentralen Helpdesk in Herzogenaurach erbracht.

2.3 Application Support

ProLeiT bietet Unterstützung für kundenspezifische Anwendungen der Plant iT / brewmaxx Software gemäß folgender Regelung:

- Engineering durch ProLeiT:
Der Application Support kann Incident-, Problem- und Change-Management beinhalten (siehe Anlage C).
- Engineering durch Drittanbieter:
Der Application Support beinhaltet ausschließlich das Incident Management.
Die Bearbeitung der Kundenanfrage erfolgt gemäß Kapitel 2.1 und wird vom zentralen Helpdesk in Herzogenaurach erbracht. Eine andere Regelung (z. B. Erbringung der Leistung durch Tochtergesellschaft an einem anderen Standort) muss in Anlage A – Kapitel 7 beschrieben werden.

2.4 Business Continuity

ProLeiT unterstützt seine Kunden bei der Entwicklung von Strategien, technischen Maßnahmen und Prozessen, um den kontinuierlichen Betrieb bzw. die schnelle Wiederaufnahme des Betriebs des Kundensystems nach einer Störung zu ermöglichen.

2.4.1 Remote Einwahl

2.4.1.1 Leistungsumfang

Der Remote Access umfasst folgende Leistungen:

- Betrieb einer zentral gemanagten Einwahlumgebung mit aktuell gepatchtem Betriebssystem und Virenschutz im Hause ProLeiT
- Initiale Einrichtung und Dokumentation der Remote-Einwahl zum Kundensystem
- Sicherstellung der Funktion der Remote-Einwahl zum Kundensystem mittels regelmäßiger Verbindungstests (2x jährlich)
- Folgende Punkte in Bezug auf die Remoteeinwahl werden im Anlage A vereinbart:
 - Einwahlmethoden
 - Software für Fernzugriff
 - Accounts (Ggf. personenbezogen)

2.4.1.2 ProLeiT Standardeinwahl

Die aktuell unterstützten Standards sind auf der ProLeiT Support Website <http://www.proleit.de/support.html> veröffentlicht.

2.4.1.3 Sondereinwahl

Als Sondereinwahl zählen alle abweichenden Einwahlmöglichkeiten (siehe Punkt 2.4.1.2)

Der Einsatz der hier aufgeführten Konstellationen muss im Einzelfall von ProLeiT geprüft werden und erfordert die explizite Zustimmung durch ProLeiT.

Änderungen der Einwahl müssen zwischen ProLeiT und dem Kunden unverzüglich abgestimmt werden.

2.4.2 Präventive Services

ProLeiT bietet seinen Kunden Services an, die das Risiko eines Produktionsausfalls minimieren.

2.4.2.1 Remote Health Check

ProLeiT überprüft den Anlagenzustand mittels eines Remote Health Checks. Die Ergebnisse werden in einem Health Check Report zusammengefasst und dem Kunden übermittelt. Der Health Check per Remote Access erfolgt während der ProLeiT Geschäftszeit (nach vorheriger Absprache mit dem Betreiber) einmal pro Kalenderjahr.

Sollten Leistungen nicht oder nicht vollständig von ProLeiT erbracht worden sein, aus Gründen die ProLeiT nicht zu verantworten hat, besteht kein Recht auf Kompensation.

Für nicht von ProLeiT projektierte brewmaxx / Plant iT Software wird nach Beginn des SLAs eine Bestandsaufnahme durchgeführt. Die Ergebnisse und Maßnahmen werden in einem System Check Report zusammengefasst und dem Kunden übermittelt. Diese Bestandsaufnahme ersetzt im ersten Vertragslaufjahr den durchzuführenden Remote Health Check.

Leistungsumfang

Der Remote Health Check beinhaltet die folgenden Leistungen für die in **Anlage A** benannten Komponenten:

- Server
 - Festplattenkapazität überprüfen
 - Arbeitsspeicher- und CPU-Auslastung prüfen

- Auswertung der Log-Dateien (Windows-Event-Logs und ProLeiT-Logs)
- Konsistenzprüfung der Datenbanken
- Prüfung der Archivierungsfunktion
- Prüfung der Uhrzeitsynchronisation zwischen Server und SPS(en)
- Prüfung der parametrisierten Verbindungen zwischen Server und SPS(en)
- Durchführung eines Basic Backups, siehe Kapitel 2.4.3 Basic Backup
- Hardwarediagnose mittels Softwaretools des Herstellers (z. B. HP Management Tools, Dell Server Administrator u. a.)
- Erfassung und Protokollierung der installierten ProLeiT Software
- Diagnose der eingesetzten Redundanz- und / oder Virtualisierungslösungen (z. B. Stratus Avance, Stratus ft), sofern von ProLeiT geliefert
- Ermittlung der Indexfragmentierung
- Prüfung der Ausführungszeiten von SQL-Abfragen
- Prüfung der Ausführungszeiten von Agenten-Jobs
- Kontrolle des Datenvolumens
- Ermittlung des Optimierungsbedarfes für SQL-Abfragepläne
- Engineeringstation
 - Funktionsprüfung der Engineeringumgebung (Step7, ProLeiT Software)
- SPS
 - Überprüfung des Speicherplatzes
 - Überprüfung der Zykluszeit
 - Auswertung des SPS-Diagnosepuffers
- Erstellung eines standardisierten Health Check-Reports:
 - Der Health Check-Report wird insbesondere folgende Informationen enthalten:
 - Auflistung aller festgestellten Werte zu Speicherbelegungen, Zykluszeiten usw.
 - Auflistung aller festgestellten Fehler, Probleme und Gefahren mit Angabe von Hinweisen zur Beseitigung
 - Zusammenfassende Beurteilung der Verfügbarkeit des Prozessleitsystems im Hinblick auf einen störungsfreien Produktionsbetrieb
 - Hinweise auf mögliche Maßnahmen zur Erhöhung der Verfügbarkeit des Prozessleitsystems
 - Das Health Check-Protokoll wird, wenn möglich, um Screenshots aus dem System Monitoring erweitert (z.B. Entwicklung des verwendeten Speichers, CPU-Auslastung, ...)

Workstations sind nicht Gegenstand des Health Checks.

Abhängig von den Ergebnissen sind in Absprache mit dem Anlagenbetreiber ggf. änderungsrelevante Maßnahmen (z.B. Re-Indizierung / Re-Build von Indizes) zur Optimierung vorzusehen. Diese werden über Changes erfasst und bearbeitet.

2.4.2.2 On-Site Health Check

Der Health Check vor Ort erfolgt während der ProLeiT Geschäftszeit (nach vorheriger Absprache mit dem Betreiber) und beinhaltet zusätzlich zu den in Kapitel 2.4.2.1 aufgeführten Leistungen die folgenden Leistungen:

- Sichtprüfung des Servers, der Engineeringstation und der SPS(en)
- Überprüfung und Erneuerung der Pufferbatterien der SPS(en)

2.4.2.3 System Monitoring

Aufgrund der immer komplexer werdenden IT-Infrastruktur setzt ProLeiT Monitoring-Lösungen ein. Das System Monitoring macht das Betriebsverhalten einer IT-Infrastruktur und ihrer einzelnen Komponenten transparent. Es liefert Informationen über den Momentanzustand, zur Historie, zeigt Trends und Tendenzen auf und alarmiert die Systemverantwortlichen beim Eintreten kritischer Situationen.

Leistungsumfang bei lokalem System Monitoring

Der Kunde erhält via Webfrontend lesenden und rein informativen Zugriff auf das System Monitoring. Das System Monitoring wird lokal beim Kunden installiert. Er kann somit 24/7 den Status seiner Systeme beobachten, historische Daten recherchieren und aufgelaufene Warnungen und Alarmmeldungen einsehen. Das lokale System Monitoring versendet keine Warn- bzw. Alarm-Benachrichtigungen via Email. Die folgenden Leistungen sind beim Betrieb des System Monitorings als lokale Instanz enthalten:

- Vorkonfiguration und Bereitstellung der Software-Appliance durch ProLeiT
- Installation, Konfiguration und Test des Systems
- Initiale anlagenspezifische Konfiguration von Warn- und Alarmschwellen der enthaltenen Checks
- Eine einmalige Nachjustierung der Warn- und Alarmschwellen

Das System Monitoring stellt dann folgende Funktionen bereit:

- Überwachung der vorkonfigurierten Checks
- Gesamtüberblick über den Status der wichtigsten Systemfunktionen in einem Dashboard
- Übersichten und Statistiken über die Auslastung der angebotenen Komponenten
- Langzeittrends von Daten

Leistungsumfang bei System Monitoring als Managed Service

Zusätzlich zu den zuvor beschriebenen Leistungen werden folgende Leistungen von ProLeiT erbracht, wenn es eine direkte Anbindung des Kundensystems per Site-to-Site gibt:

- Proaktives Erkennen von Störungen, Ausfällen und Überlastsituationen in Soft- und Hardware
- E-Mail-Alarmierung an monitoring@proleit.com
- Überführung der Störungsmeldung in das Event Management von ProLeiT
- Überwachung der Betriebsbereitschaft des System Monitorings durch ProLeiT
- Der Kunde wird ebenfalls automatisch per E-Mail vom System Monitoring alarmiert und kann weitere Schritte zur Störungsbehebung veranlassen

Optionale Leistungen

Das System Monitoring als Managed Service kann um die folgenden Leistungen erweitert werden:

- Überwachung weiterer IT-Dienste
- Überwachung weiterer Hardware, wie z. B. USV oder eingesetzter Netzwerkkomponenten (Switches), sofern Checks des Herstellers verfügbar sind oder von ProLeiT entwickelt wurden. Eine aktuelle Liste der möglichen Überwachungen (Checks) kann auf der Produkt-Webseite eingesehen werden (<https://checkmk.de>)

Diese optionalen Leistungen werden in der Anlage A– Kapitel 7 vereinbart.

Technische Rahmenbedingungen

Die System Monitoring-Lösung „checkMK“ wird auf einer Appliance zusätzlich zum PLS / MES betrieben (d. h. eigenständiger virtueller Server).

Folgende Voraussetzungen sind auf Kundenseite erforderlich:

- Bereitstellung der notwendigen Gerätedaten, Netzwerkadressen und Informationen
- Bereitstellung der Ressourcen für den Betrieb der Appliance, sofern diese auf der IT-Infrastruktur des Kunden betrieben wird
- Feste interne IP-Adresse für die Monitoring Appliance
- Zugriffsrechte der Monitoring-Lösung auf die zu überwachenden Systeme (z. B. SNMP oder ESX-User mit ausreichenden Berechtigungen)
- Zugriff der Monitoring Appliance auf einen Mailserver
- DNS-Server und Zeitserver

- Lesender Zugriff auf die Schnittstellen der zu überwachenden Systeme
- Unterstützung durch die Kunden-IT bei Konfiguration, Update und Installation der Monitoring-Lösung

Einschränkungen des System Monitorings

Das System Monitoring überwacht die Komponenten des von ProLeiT gelieferten PLS / MES sowie ggf. beigestellte IT-Infrastruktur, Hardware und Drittsoftware, die Bestandteil des PLS / MES sind. Die reine Überwachung bedeutet keine hundertprozentige Garantie, alle Ausfälle zu erkennen. Sie kann aber einen entscheidenden Beitrag zur Erhöhung der Verfügbarkeit und zum Schutz vor Systemausfällen und Performanceeinbußen leisten.

Wird die IT-Infrastruktur durch den Kunden bzw. ein Drittunternehmen beigestellt, beschränkt sich der Leistungsumfang von ProLeiT lediglich auf die Erstanalyse mit anschließender Beratung. Für die Störungsbehebung sind der Kunde bzw. das Drittunternehmen verantwortlich.

Die Verantwortung für den Betrieb der Produktionsanlage verbleibt uneingeschränkt beim Kunden und ProLeiT kann für einen Schaden, der durch das Ausbleiben einer Meldung durch das System Monitoring entsteht, nicht haftbar gemacht werden.

Änderungen und Erweiterungen

Aufwendungen für Anpassungen von Checks und Erweiterungen der System Monitoring-Funktionen sowie das Ändern von Warnschwellwerten werden als Change (RfC) oder Service Request behandelt und verrechnet.

2.4.2.4 Event Management

Das Event Management stellt sicher, dass Konfigurationselemente (CIs) und Services kontinuierlich überwacht werden. Der Prozess filtert und kategorisiert Events, um ggf. geeignete Maßnahmen einzuleiten.

- Zu messende CIs und deren Grenzwerte werden mit dem Kunden definiert
- Auftretende Events werden durch Monitoring Systeme erkannt, protokolliert und nach einer Erstkorrelation an den Helpdesk weitergeleitet.
- Dort erfolgt eine Second Level Korrelation
- Ggf. eine Überführung in nachgelagerte Prozesse zur Behebung von Störungen oder Einleiten von Changes / Problems

Das Event Management wird ausschließlich während der Geschäftszeit von ProLeiT am Standort Herzogenaurach (Bayern, Deutschland) erbracht (siehe Kapitel 1.9 Geschäftszeit). Außerhalb der Geschäftszeit bieten die Daten des System Monitorings zusätzliche Informationen, um einen Major Incident zu lösen.

2.4.2.5 Kundenspezifische System Monitoring Reports

Das System Monitoring kann automatisiert erstellte und vorkonfigurierte Reports an eine beliebige E-Mail-Adresse versenden. Ein solcher Report kann mehrere grafische Auswertungen von beliebigen Checks enthalten. Der Report wird als pdf-Datei automatisch zu einem gewünschten Zeitpunkt versandt (z.B. jeden Tag um 7:00). Ein typisch eingesetzter Report ist die Zusammenstellung von Daten, die die Stabilität eines Produktionsumfelds beschreiben. Die Konfiguration der Reports wird über einen Service Request verrechnet.

2.4.3 Basic Backup

Zu Vertragsbeginn wird eine Projektsicherung auf den Servern der ProLeiT abgespeichert. Diese beinhaltet die Anlagenkonfiguration (Datenbank-Sicherung) und das SPS-Projekt. Sie beinhaltet keine Bewegungs- und Archivdaten.

Bei jedem Health Check (siehe Kapitel 2.4.2.1) wird erneut ein Basic Backup durchgeführt und auf dem Kundenserver abgelegt.

2.4.4 Advanced Backup Disaster Recovery Concept

ProLeiT bietet seinen Kunden Beratung und Unterstützung bei Backup & Disaster Recovery an. Ausgehend von den Kundenanforderungen bezüglich maximal zulässiger Ausfallzeiten und maximal zulässiger Datenverluste wird ein Konzept zur schnellen Wiederherstellung des Betriebs erstellt. Als Ergebnis wird ein individuelles, auf die IT-Infrastruktur und IT-Prozesse des Kunden abgestimmter Service entwickelt.

Das Konzept beinhaltet folgende Punkte:

- Erstellung eines Konzeptes basierend auf den Kundenanforderungen, z. B.
 - Werte für RTO (Recovery Time Objective) und RPO (Recovery Point Objective)
 - Festlegung der IT-Architektur: Shared Backup oder dedizierte Umgebung
 - Umfang und Häufigkeit von Disaster-Recovery-Tests
 - Anforderungen an das Reporting des Backups
 - Festlegung der einzusetzenden Software / Hardware
- Optional Umsetzung des Konzeptes
 - Optional Bereitstellung einer Testumgebung zum Nachstellen des Kundensystems (siehe Kapitel 2.5.4)

Die genauen Vereinbarungen werden in **Anlage A**– Kapitel 7 festgelegt.

2.4.5 Patch Management

ProLeiT bietet seinen Kunden Unterstützung bei der regelmäßigen Aktualisierung des Kundensystems durch Security Patches für Microsoft Betriebssysteme, um die IT-Sicherheit zu gewährleisten. Dies umfasst die Bereitstellung von individuellen Patchlisten, Beratungsleistungen bis hin zu individuell auf die Anlagenkonfiguration zugeschnittenen Handlungsempfehlungen.

Der ProLeiT-Leistungsumfang beinhaltet Beratungsleistungen zu

- Security Patches für Microsoft Betriebssysteme
- Security Patches für Microsoft SQL Server
- im Kontext mit der eingesetzten Plant iT / brewmaxx Systemsoftware.

Für die Einführung eines Patch Management Prozesses empfiehlt ProLeiT folgende Voraussetzungen und Vorgehensweisen.

Voraussetzungen:

- Geeignete Werkzeuge für:
 - Ermittlung des Patchbedarfes (z.B. durch einen Vulnerability Scanner)
 - Automatisierte Verteilung von Patches (z.B. Matrix42 Empirum)
- eingeführter Change Prozess
- Ein Advanced Backup Disaster Recovery Plan ist definiert und erfolgreich eingeführt (siehe Kapitel 2.4.4 Advanced Backup Disaster Recovery Concept)
- Die verwendeten Produkte (z.B. Microsoft SQL Server, Microsoft Windows, ...) sind im Support Lifecycle und kompatibel mit der verwendeten Plant iT / brewmaxx-Version gemäß den ProLeiT Release Notes

Vorgehensweise und Annahmen:

- Innerhalb eines Workshops wird ein Gesamt-Konzept erarbeitet, in dem Abläufe, Aufgaben und der zeitliche Rahmen definiert werden. Der Workshop wird von ProLeiT organisiert und erstreckt sich über acht Stunden, mit Vertretern der ProLeiT Applikations- und IT-Spezialisten.
- Die Zeitfenster für die Verteilung der Patches (Kern-Wartungszeitfenster) werden gemeinsam zwischen dem Kunden und ProLeiT abgestimmt (Patch Kalender). Der Kunde stellt sicher, dass die Patches in den vereinbarten Zeitfenstern ausgerollt werden können. In Abhängigkeit von den zu patchenden Items erfordert dies ggf. Downtimes für die Produktion.
- Klärung des Umfangs der zu patchenden Systeme / Geräte (ProLeiT Lieferumfang oder darüberhinausgehend). Dies erfordert den Einsatz einer Configuration Management Database (CMDB) für die beim Kunden eingesetzten Hardware und Software Items. Die Aktualisierung dieser Datenbank liegt in der Verantwortung des Kunden.
- Basierend auf der von ProLeiT veröffentlichten Patch Matrix für Plant iT / brewmaxx Software im Zusammenspiel mit Microsoft Betriebssystem und SQL Server spricht ProLeiT Patch-Empfehlungen für die jeweilige Kundenanlage aus. Diese Empfehlungen, resultierend aus einem generellen Smoke Test, beinhalten vor allem Security Patches. Der Kunde leitet aus dieser Empfehlung seinen Bedarf zum Patchen seiner Systeme ab.
- Unterliegt die verwendete Plant iT / brewmaxx Version gemäß dem ProLeiT Lifecycle dem On-Demand-Support, wird der anlagenspezifische Test um die Bestandteile des Smoke Tests erweitert.
- Vor dem Rollout auf dem produktiven System ist ein Test der Patches im Testsystem (siehe Kapitel 2.5.4 Testsystem und virtuelle Fabrik) durchzuführen. Hierfür müssen je Testfall entsprechende Testszenarien und Fallback-Szenarien erarbeitet und dokumentiert werden. Nur nach erfolgreichem bestandenen Test darf der Rollout auf das produktive System erfolgen.
- Die Freigabe für den Rollout auf das produktive System erfolgt durch den Kunden.
- Der Rollout auf das produktive System wird vom Kunden durchgeführt.
- Nach dem Rollout sind entsprechende Funktionstest durch den Kunden vorzunehmen (siehe SLA Kapitel Tests). Bei negativem Funktionstest ist vom Kunden zu entscheiden, ob das Fallback-Szenario angewendet wird.
- Nach dem Rollout steht dem Kunden, während der Geschäftszeit, ein anlagenerfahrener ProLeiT Mitarbeiter innerhalb einer Hypercare-Phase für acht Stunden remote zur Verfügung, um auftretende Punkte direkt und effizient klären zu können.
- Die Produktionsfreigabe nach dem erfolgreichen Funktionstest erfolgt durch den Kunden.

Abgrenzung:

- Minor und Major Releases (z. B. Betriebssystem-Updates oder Plant iT /brewmaxx Versions-Upgrades) sind nicht Bestandteil des Patch Managements, sondern sind als Projekte abzuwickeln
- Das Patchen von Drittsoftware ist nicht enthalten, außer eine spezifische Software wurde im Leistungsumfang des Patch Managements benannt, siehe **Anlage A**– Kapitel 7.
- Aus dem Patch Management lassen sich keine Gewährleistungsansprüche ableiten

2.4.6 Hardware Support

ProLeiT bietet Unterstützung für im Lieferumfang von ProLeiT enthaltene Hardware.

Darunter fallen z. B: Herstellersupport von HP, Dell, Stratus oder VMware. Voraussetzung ist ein gültiger Servicevertrag mit dem Hersteller des jeweiligen Produkts. Der Kunde ist für die ggf. notwendigen Verlängerungen des Servicevertrags für das jeweilige Produkt verantwortlich, alternativ kann diese Leistung als Sondervereinbarung aufgenommen werden, siehe **Anlage A**– Kapitel 7.

ProLeiT bietet beispielsweise als Stratus Reseller definierte Services an, so dass der ProLeiT Helpdesk als erster Ansprechpartner bei Störungen fungiert.

2.4.7 OT Cybersecurity First Level Assessment

Bedarf im geschäftlichen Umfeld

Unternehmen arbeiten mehr denn je daran, ihren Betrieb zu modernisieren und zu digitalisieren, um mehr Transparenz und Effizienz aus ihren OT-Assets (OT: Operative Technologie) zu gewinnen. Dennoch stufen viele Organisationen ihr Steuerungsnetzwerk als unbedeutendes Risiko ein. Jüngste Cyber-Vorfälle und Angriffe sind ein Beweis dafür, dass OT-Angreifer weitaus raffinierter, heimtückischer und dreister sind als je zuvor. Und abgesehen von böswilligen Angriffen sind viele OT-Sicherheitsprobleme zufälliger Natur.

Das OT Cybersecurity First Level Assessment von ProLeiT bewertet die Stärke der OT-Cybersicherheits-Abwehr und -Richtlinien der Kunden und bietet Anleitungen, um Führungskräften zu helfen, umsichtige Cybersicherheitsentscheidungen zu treffen und sicherzustellen, dass sich Investitionen in Cybersicherheit in Form von erhöhtem Bewusstsein und Vorbereitung gegenüber Angriffen auszahlen.

Lösung

Das OT Cybersecurity First Level Assessment bietet Kunden eine nicht-invasive Analyse ihres OT-Cybersicherheitsprofils unter der Leitung der Cybersicherheit-Experten von Schneider Electric. Der Service liefert einen klaren Überblick über den Cyberstatus des Kunden und einen Weg zur Erreichung der Cybersicherheitsziele, unabhängig davon, ob es sich um die Befolgung von Best Practices der Branche oder die Einhaltung von Richtlinien und Standards wie ISA-62443, NIST, NERC CIP, CFATS und ISO27001 handelt.

Nach Abschluss der Bewertung liefern die Prüfer einen OT-Cybersicherheit-Bericht mit Abhilfesritten, um Kunden eine umsetzbare Roadmap zur Verbesserung ihrer OT-Cybersicherheit zu liefern.

Diese Bewertung ist herstellerunabhängig und wird einmal jährlich durchgeführt. So wird die OT-Cybersicherheitslage kontinuierlich verbessert.

Dieser Service zielt auf die komplette OT ab und betrachtet nicht nur das Plant iT / brewmaxx System.

Lieferumfang

Die beschriebene Lösung setzt sich aus 2 Schlüsselementen zusammen:

1. Telefonisches Interview zur Cybersicherheitslage
 - Planung - Die Ziele des Kunden werden erfasst, und es werden Einsatzregeln festgelegt.
 - Feststellungsverfahren - Durchführung virtueller Interviews, um potenzielle Schwachstellen, schwache Bereiche und Sicherheitslücken zu identifizieren. Es ist kein Zugang zum Standort erforderlich.
 - Zeitlicher Umfang ca. 4 Stunden
2. OT Cybersicherheit Bericht
 - Cyber-Einstufungsprofil und Empfehlungen für Abhilfemaßnahmen

Details

Ziel ist es, Kunden ein Profil der Cybersicherheitslage von Steuerungssystemen zu liefern, das auf der Expertenanalyse von Daten basiert, die über Interviews gesammelt wurden. Innerhalb des Interviews werden folgende Punkte thematisiert:

- Netzwerkarchitektur
- PCS-Systemkomponenten
- Cybersicherheitsverfahren und -richtlinien
- Physische Sicherheitsverfahren
- Cyber-Schulungsniveau von PCS-Personal
- Dokumentierte Verfahren zur Reaktion auf Vorfälle
- Lifecycle-Management
- Rollenbasierte Sicherheitspraktiken

Die Interviews werden in der Regel virtuell und innerhalb eines einzigen Arbeitstages durchgeführt. Nach Abschluss der Interview-Komponente der Überprüfung erstellen und liefern die Cybersicherheit-Experten von Schneider Electric einen zusammenfassenden Bericht mit den Cybersicherheit-Ergebnissen, Lücken und empfohlenen Abhilfemaßnahmen für das OT-Steuernetzwerk auf Grundlage der ISA 62443-Standards. Die Ressourcen von Schneider Electric sind mit ihrem Hintergrund und ihrer fortgeschrittenen Ausbildung im Bereich der betrieblichen Cybersicherheit sowie ihrer weitreichenden Branchenerfahrung mit Steuerungssystemen und elektrotechnischen Prozessen bestens für die Durchführung dieser Dienstleistung qualifiziert.

Folgende Liste definiert Schweregrade, die im gesamten Dokument zur Beurteilung der Auswirkungen verwendet werden:

- **Kritisch:**
Eine Ausnutzung ist einfach und führt normalerweise zu einer Kompromittierung auf Systemebene. Es wird empfohlen, einen Aktionsplan zu erstellen und sofort zu patchen.
- **Wichtig:**
Eine Ausnutzung ist schwieriger, kann aber zu erhöhten Rechten und möglicherweise zu Datenverlusten oder Ausfallzeiten führen. Es wird empfohlen, einen Aktionsplan zu erstellen und so schnell wie möglich zu patchen.
- **Mäßig:**
Schwachstellen existieren, sind aber nicht ausnutzbar oder erfordern zusätzliche Schritte. Es wird empfohlen, einen Aktionsplan zu erstellen und Patches zu installieren, nachdem die Probleme mit hoher Priorität behoben wurden.
- **Niedrig:**
Die Schwachstellen sind nicht ausnutzbar, würden aber die Angriffsfläche einer Organisation verringern. Es wird empfohlen, einen Aktionsplan zu erstellen und während des nächsten Wartungsfensters zu patchen.

Der OT-Cybersicherheit-Report enthält Abhilfeempfehlungen für die Feststellungen. Diese Behebungsempfehlungen werden über Changes erfasst und verarbeitet.

Voraussetzungen

Um sicherzustellen, dass die Prüfer einen vollständigen und umsetzbaren zusammenfassenden Bericht liefern können, müssen diese so viel wie möglich über die OT-Systeme des Kunden erfahren, bevor sie Interviews durchführen. Daher sollten die folgenden Informationen, sofern verfügbar, bereitgestellt werden:

- OT-Netzwerkdiagramm mit PCS-Layers/Zones und Beschriftungen, die die Standorte der kritischen Anlagen im Netzwerk zeigen.
- Identifizierung von Personal, das mit dem Aufbau und der Verwaltung von OT-Netzwerken am besten vertraut ist und detaillierte technische Fragen zu den im Kundennetzwerk verwendeten OT-Geräten/Assets beantworten kann.
- Informationen zur aktuellen Cybersicherheitspolitik, einschließlich vorhandener Cybersicherheits-Tools/Technologien, wichtiger Standards/Ziele und Rollen/Zuständigkeiten im Zusammenhang mit einem vorhandenen Cybersicherheitsprogramm.

Liefergegenstand

Nach Abschluss der Interview-Komponente der Bewertung erstellen und liefern die Cybersicherheit-Experten von Schneider Electric einen Cybersicherheit-Bewertungsbericht mit Erkenntnissen zu den evaluierten Cybersicherheit-Richtlinien, Lücken und empfohlenen Abhilfemaßnahmen auf Grundlage der ISA 62443-Standards. Dieser Bericht enthält eine prioritätenbasierte Liste mit umsetzbaren Erkenntnissen zur Cybersicherheit und Expertenempfehlungen, die auf dem Steuerungsnetzwerk des Kunden und den ISA 62443-Standards basieren.

2.4.8 Installation Services

ProLeiT hält geschultes Personal für die Installation und den sicheren Betrieb von Hardware und Software vor.

Bei Störungen oder einem Ausfall eines Geräts unterstützt ProLeiT mit der entsprechenden Fachexpertise unter Beachtung der jeweiligen Herstellervorgaben bei der Installation, Konfiguration und dem Test der Hardware.

ProLeiT unterstützt bei der Installation der notwendigen Software. Dies beinhaltet beispielsweise die Plant iT / brewmaxx Basisinstallation, die für den Betrieb erforderliche Anwendungssoftware bis hin zur kompletten Wiederherstellung von Daten aus Backups.

2.5 Business Improvement

ProLeiT bietet seinen Kunden Services an, um die Effektivität und Effizienz von Geschäftsprozessen stetig zu verbessern.

2.5.1 Service Manager

ProLeiT bietet seinen Kunden eine regelmäßige und individuelle Betreuung durch einen Service Manager als dedizierten Ansprechpartner. Dieser nimmt die folgenden Aufgaben wahr:

- Dedizierter Ansprechpartner für alle Themen im Bereich Service Management
- Online-Besprechung mit dem Ansprechpartner des Kunden
 - Überprüfung der Bearbeitung aller offenen Tickets des Kunden.
 - Erstellung von Statistiken und Übersichten
 - Nachweis der erbrachten SLA Leistungen
- Möglichkeit der Incident-Eskalation über den Service Manager
- Besprechung einzelner Incident-/ Problem-Reports
- Veranlassung der Untersuchung komplexer oder mehrfach aufgetretener oder über einen längeren Zeitraum bestehender Probleme mit dem Ziel, nachhaltige Lösungen zu erarbeiten (Problem Management)
- Führung der Kommunikation im Bereich Problem und Change Management, falls im Vertrag enthalten
- Veranlassung von Vertragsanpassungen in Absprache mit dem ProLeiT Key-Account / Vertriebsbeauftragten z.B. bei neuen Kundenanforderungen, Änderungen von Mengengerüsten, Über- / Unterschreitung von Kontingenten

2.5.2 Problem Manager

Der Problem Manager arbeitet in enger Abstimmung mit dem Service Manager. Er ist mit den Produktionsprozessen des Kunden und der Projektierung der Plant iT/brewmaxx Anwendung vertraut. Er dient dem Kunden als technischer Ansprechpartner zur nachhaltigen Lösung von auftretenden Störungen in einem an ITIL angelehnten Standardprozess. Das Aufgabengebiet umfasst:

- Überwachung der nachhaltigen Lösung von Incidents
- Proaktive Untersuchung komplexer oder mehrfach aufgetretener oder über einen längeren Zeitraum bestehender Probleme mit dem Ziel, nachhaltige Lösungen zu erarbeiten
- Erstellung von Workaround-Beschreibungen zur Lösung bekannter Störungen (Known Errors)
- Fachlicher Austausch mit der Entwicklungs- und der Projektierungsabteilung von ProLeiT
- Erstellen von Statistiken und Reports

2.5.3 Change Manager

ProLeiT bietet seinen Kunden die Bearbeitung von Changes an. Diese können konkrete Änderungsanfragen sein oder sich aus anderen Serviceleistungen ergeben.

Der Change Manager entwickelt in Abstimmung mit dem Kunden den Prozess zur Implementierung von Changes auf das Produktivsystem des Kunden.

Der Change Manager bewertet die erforderlichen oder gewünschten Anpassungen nach den folgenden Kriterien: Machbarkeit, Aufwandsabschätzung, Testbeschreibungen und Risikoabschätzung. Ein bewerteter Change wird als Change Request (CR) an den Kunden übermittelt.

Nach entsprechender Freigabe und Beauftragung durch den Kunden erfolgt die Implementierung des Changes gemäß dem abgestimmten Prozess für die jeweiligen Kategorien des Change, siehe Kapitel 1.6. Der Change Manager organisiert die dafür erforderlichen Maßnahmen.

Sämtliche Aufwendungen (siehe oben) des Change Managements werden über ein Stundenkontingent, siehe Kapitel 3.4, abgerechnet. Die Kontingentgröße wird in Anlage A – Kapitel 7 definiert.

2.5.4 Testsystem und virtuelle Fabrik

ProLeiT bietet seinen Kunden an, das Produktivsystem in einer vergleichbaren Engineeringumgebung nachzubilden.

In diesem System können Changes vorab getestet werden. Mögliche Szenarien können in einer realitätsnahen Umgebung getestet werden. Das System kann um zusätzliche Hard- und Software erweitert werden, um eine Art virtuelle Fabrik zu implementieren.

Ein typischer Aufbau eines Testsystems beinhaltet die Funktionalitäten des Datenbank-Servers, der SPS, mindestens einer Bedienstation sowie ggf. zugehörige Peripherie (z. B. Scanner, Karten- oder Chiplesegeräte).

Die dafür erforderliche Infrastruktur sowie der detaillierte Umfang von Services werden in an **Anlage A** – Kapitel 7 festgelegt.

2.5.5 Software-Optimierungen vor Ort

ProLeiT bietet seinen Kunden an, kleinere Optimierungen der Software vor Ort durchzuführen. Meist wird diese Optimierung im zeitlichen Zusammenhang mit einem Health Check On-Site (siehe Kapitel 2.4.2.2 On-Site Health Check) durchgeführt. Darunter zählen beispielsweise Verbesserungen der Bedienerführung oder die Optimierung der automatisierten Prozessabläufe.

Ziel ist dabei, einen Dialog mit dem Bedienpersonal zu eröffnen und Anpassungen zur Optimierung vor Ort vorzunehmen. Jegliche Anpassungen erfordern eine Spezifikation, die Rückführung in die Anlagendokumentation und eine anschließende Abnahme.

Es gelten die Bestimmungen gemäß Kapitel 5

Mitwirkungspflicht des Kunden. ProLeiT empfiehlt dafür einen standardisierten Change Prozess.

2.5.6 Knowledge Management for Applications

ProLeiT bietet seinen Kunden an, spezielle Wissensartikel auf einer vereinbarten Plattform zu erstellen. Diese Wissensartikel könnten Lehrvideos, Handlungsempfehlungen zur Störungsbehebung, Entscheidungsbäume etc. umfassen. Der Umfang der Leistungen wird in der Anlage A – Kapitel 7 vereinbart.

2.5.7 Training

ProLeiT bietet seinen Kunden Schulungen für verschiedene Zielgruppen wie z. B. Administratoren, Projektierer und Bediener an.

2.5.7.1 Standardschulungen

Die Standardschulungen werden am Standort Herzogenaurach in der aktuellen Plant iT / brewmaxx-Version in deutscher und englischer Sprache angeboten. Das aktuelle Schulungsangebot ist auf <https://www.proleit.de/training.html> veröffentlicht.

2.5.7.2 Kundenspezifische Schulungen

Auf Anfrage können kundenspezifische Schulungen (z.B. Bedienschulungen vor Ort) von ProLeiT angeboten werden. Kundenspezifische Schulungen können beispielsweise beim Kunden, in der speziellen Anwendung des Kunden sowie in anderen Sprachen durchgeführt werden.