

Anforderungscheckliste »Sichere Fernwartung« für KMU

Kurzfassung

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-
Digital



Inhalt

1. Wofür Sie diese Checkliste brauchen.....	2
2. Warum Fernwartung besonders gut geschützt sein muss	3
3. Schnellprüfung: Zehn Fragen, die jede Lösung bestehen muss	4
4. Weiterführende Informationen	6
5. Quellen und Herleitung	7
6. Glossar	7
7. Förderhinweis	8

1. Wofür Sie diese Checkliste brauchen

Fernwartung ist eines der mächtigsten Werkzeuge in Ihrem Unternehmen: Sie verbindet einfachen Zugang mit weitreichenden Rechten. Genau deshalb ist sie auch für Angreifer eines der begehrtesten Ziele. Diese Checkliste übersetzt die Ergebnisse aus Interviews, Expertentipps, Normen und realen Vorfällen in prüfbare Anforderungen, an denen Sie jede Fernwartungslösung messen können, egal ob Sie eine neue beschaffen oder eine bestehende bewerten.

Drei Anwendungsfälle:

1. **Neubeschaffung:** Arbeiten Sie die Schnellprüfung (Abschnitt 3) durch und bewerten Sie die Kandidaten anschließend anhand der erweiterten Anforderungsliste in der separaten Datei 09b.
2. **Bestandslösung bewerten:** Prüfen Sie zuerst die K.O.-Kriterien aus Abschnitt 3. Besteht Ihre Lösung sie nicht, haben Sie Handlungsbedarf, unabhängig von allem anderen.
3. **Dienstleister-Zugriffe auf Ihre Maschinen:** Wenn nicht Sie fernwarten, sondern ein Hersteller oder Dienstleister auf Ihre Anlagen zugreift, ist Abschnitt 5.9 der Datei 09b Ihr Kernkapitel.

Welcher Fall betrifft Sie? Die *Datei 09b* ordnet drei Fällen die jeweils einschlägigen Kapitel zu: **A** – Sie fernwarten Ihre eigenen Geräte (IT-Support, Server, Arbeitsplätze); **B** – Externe (Maschinenhersteller, Dienstleister) fernwarten Ihre Maschinen und Anlagen; **C** – Sie sind selbst Dienstleister und fernwarten Systeme Ihrer Kunden. Die Fälle schließen sich nicht aus; viele KMU treffen mehrere gleichzeitig zu.

2. Warum Fernwartung besonders gut geschützt sein muss

Sie brauchen diese Checkliste nicht, weil Fernwartung neu oder grundsätzlich schlecht ist, sondern weil sie gleichzeitig Ihr wichtigstes Sicherheitswerkzeug und der kürzeste Weg in Ihr Unternehmen sein kann. Neun reale Vorfälle zeigen das Muster:

Vorfall	Was passierte	Die Lücke, die es ausnutzte
SolarWinds / SUNBURST, 2020	Staatliche Angreifer kompromittierten die Build-Pipeline des Herstellers; rund 18.000 Kunden — darunter US-Behörden — installierten trojanisierte, digital signierte Updates	Kompromitierte Build-/Update-Pipeline des Herstellers (Lieferkettenangriff)
Wasserwerk Oldsmar (Florida), Februar 2021	Unbefugte erhöhten über eine Fernzugriffsverbindung die Laugen-Dosierung der Trinkwasseraufbereitung; das Bedienpersonal bemerkte und korrigierte den Eingriff sofort	Schwache Passwörter und veraltetes Betriebssystem auf dem Fernzugangs-Weg; welche Fernwartungssoftware genau genutzt wurde, ist laut CISA nicht bestätigt
Kaseya VSA / REvil, Juli 2021	Erpressungssoftware wurde über die Fernwartung selbst an rund 1.500 Unternehmen verteilt (in Schweden musste ein Einzelhändler 800 Filialen schließen)	Zero-Day-Kette gegen den öffentlich erreichbaren VSA-Server; Ausbreitung über den vertrauten Verteilweg.
CISA-Warnung AA23-025A, 2022/23	Kriminelle überreden Mitarbeitende per Anruf, legale Fernwartungsprogramme zu installieren, und zwar als portable Datei ohne Installation; portables RMM entgeht oft Virenerkennung und Software-Kontrolle	Fehlende Sperrung fremder Fernwartungssoftware + fehlende Sensibilisierung
AnyDesk, Januar 2024	Eindringlinge erbeuteten Quellcode und Signaturzertifikate des Herstellers — die "Echtheitsmarke" der Software	Vertrauen in die Lieferkette des Anbieters
ScreenConnect, Februar 2024	Angriffswelle auf eine Schwachstelle mit Höchstschwergewicht (CVSS 10.0); Ausnutzung durch mehrere Ransomware-Gruppen	Verwundbare, internetseitig erreichbare Installationen
TeamViewer, Juni 2024	Staatlich agierende Angreifer (APT29) kompromitierten ein Standard-Mitarbeiterkonto im internen Netz des Herstellers	Ursache und Zugangsmethode wurden nicht offengelegt; die Netz-Trennung begrenzte die Auswirkungen auf das Produkt
BeyondTrust / US-Finanzministerium, Dezember 2024	Ein kompromittierter API-Schlüssel in der Cloud-Infrastruktur des Fernsupport-Anbieters erlaubte Angreifern, lokale Anwendungspasswörter zurückzusetzen und auf Kundensysteme zuzugreifen — betroffen auch das US-Finanzministerium (China-attribuierte Spionage)	Kompromittierter Dienstschlüssel beim Hersteller; Passwort-Reset aus der Ferne als unbemerktes Privileg
SimpleHelp RMM, Juni 2025	Ransomware-Akteure (El Dorado) nutzten die ungepatchte Pfad-Traversal-Schwachstelle CVE-2024-57727 (SimpleHelp ≤ 5.5.7) im RMM eines Abrechnungssoftware-Anbieters und kompromitierten den Anbieter und seine Kunden	Ungepatchtes, erreichbares RMM — als Bundle in Drittanbieter-Software oft gar nicht als eigenständiges Produkt erkannt

Die dokumentierten Angriffspfade lassen sich mit den Anforderungen dieser Checkliste überwiegend verhindern, begrenzen oder zumindest bemerken. Zwei Regulierungen machen das Thema zeitkritisch:

- *NIS2 (BSIG, in Kraft)*: Direkt erfasst ist nur, wer unter NIS2 fällt ("wichtige und besonders wichtige Einrichtungen"). Viele mittelständische Unternehmen erhalten sicherheitsbezogene Anforderungen aber vertraglich über die Lieferkette weitergereicht; das begründet noch keinen automatischen NIS2-Anwendungsbereich. Sicherheitsanforderungen an die Fernwartung sind ein Baustein der geforderten Risikomaßnahmen (§ 30 Abs. 2 BSIG).
- *Cyber Resilience Act (CRA, Verordnung (EU) 2024/2847)*: Meldepflichten für Schwachstellen gelten seit dem 11.09.2026; die volle Anwendung folgt ab 11.12.2027. Die Pflichten sind rollenspezifisch: Sie treffen primär die Hersteller, während Importeure und Händler eigene Prüf- und Mitwirkungspflichten haben. Als Käufer empfehlen wir, die geforderten Produkteigenschaften (z. B. signierte Updates, SBOM) heute schon als Beschaffungsanforderung einzufordern.

3. Schnellprüfung: Zehn Fragen, die jede Lösung bestehen muss

Diese zehn Fragen sind die Schnellprüfung dieser Checkliste: Fällt eine davon durch, scheidet die Lösung für den produktiven Einsatz aus, unabhängig der anderen Vorzügen. Alle Kriterien sind in der *Datei 09b* ausführlicher beschrieben.

#	Frage an den Anbieter	Erwartete Antwort
1	Wird bei aktivierter Multifaktor-Authentisierung verhindert, dass sich jemand allein mit Benutzername und Passwort an der Verwaltungskonsole anmeldet?	Ja , zusätzlich zum Passwort wird ein unabhängiger zweiter Faktor verlangt; diese Pflicht gilt auch für rein lesende Konten, sodass ein gestohlenes Passwort allein keinen Zugang ermöglicht.
2	Werden alle Verbindungen (Konsole, Sitzung, Agent) mit modernem TLS (1.2+/1.3) verschlüsselt, ohne Ausnahme und ohne unsicheren Rückfall?	Ja , sämtliche Verbindungen nutzen mindestens TLS 1.2; Zertifikate werden geprüft und Verbindungsversuche bei ungültigen Zertifikaten oder unsicheren Protokollen abgewiesen.
3	Sind die Agenten-Programme digital signiert, und meldet der Agent Manipulationen an seiner eigenen Datei?	Ja , digitale Signaturen bestätigen Herkunft und Unverändertheit der Agenten-Programme; eine Integritätsprüfung erkennt Änderungen an der Programmdatei und löst eine Meldung aus.
4	Werden alle Sitzungen protokolliert (wer, wann, von wo, auf welches Gerät, was wurde übertragen) und lassen sich die Protokolle exportieren?	Ja , alle Sitzungen werden exportierbar protokolliert; nachvollziehbar sind Konto, Zeitpunkt, Zugriffsquelle, Zielgerät sowie übertragene Daten und Dateien.
5	Beginnt eine Sitzung auf einem Mitarbeiter-PC nur nach sichtbarer Ankündigung bzw. Freigabe, und kann die betroffene Person sie jederzeit selbst beenden?	Ja , die betroffene Person erkennt vor Beginn, dass ein Fernzugriff erfolgen soll, und erteilt bei vorgesehener Freigabepflicht ihre Zustimmung; eine jederzeit erreichbare Schaltfläche beendet den Zugriff sofort.
6	Bauen die Agenten ausschließlich ausgehende Verbindungen auf, sodass keine eingehenden Firewall-Freigaben auf Ihren Geräten erforderlich sind?	Ja , der Agent stellt die Verbindung selbst nach außen her; weder eingehende Portfreigaben noch Portweiterleitungen auf die verwalteten Geräte sind erforderlich.

#	Frage an den Anbieter	Erwartete Antwort
7	Ist die Verwaltungskonsole nur aus dem Internen Netzwerk und nicht direkt und anonym aus dem Internet erreichbar?	Ja , Administratoren müssen zunächst einen authentisierten Zugang, etwa per VPN, herstellen.
8	Gibt es einen dokumentierten Notfall-Abschalter (alle Sitzungen kappen, Konto sperren, Agenten flächendeckend isolieren) und Verfahren zum Austausch aller Zugangsdaten?	Ja , eine dokumentierte Notfallfunktion ermöglicht das Trennen aller Sitzungen, Sperren von Konten und Isolieren aller Agenten; Zuständigkeiten und Verfahren zum Austausch sämtlicher Zugangsdaten sind festgelegt.
9	Werden Sicherheitsupdates getrennt von Funktions-Updates, unverzüglich, innerhalb eines genannten Supportzeitraums bereitgestellt? Sind diese bei kommerziellen Produkten vertraglich zugesagt?	Ja , Sicherheitskorrekturen lassen sich ohne ein Funktionsupgrade einspielen und werden während des benannten Supportzeitraums unverzüglich geliefert; bei kommerziellen Produkten sind diese Pflichten vertraglich festgehalten.
10	Werden Zugriffe je Gerät / je Gerätegruppe zugeteilt, sodass ein Techniker-Konto nicht automatisch auf alles zugreifen kann?	Ja , Berechtigungen folgen dem Prinzip der geringsten Rechte: Techniker erhalten nur die für ihre Aufgaben benötigten Gerätezugriffe; zusätzliche Freigaben müssen ausdrücklich zugewiesen werden.

4. Weiterführende Informationen

- **Datei 09b – Anforderungscheckliste "Sichere Fernwartung" (Erweitert):** Enthält die erweiterten Anforderungen (CL-...) nach Themenbereich gegliedert — Identität und Zugriff, Sitzungssicherheit, Agent und Endgeräte, Netzwerk-Anbindung und Infrastruktur, Protokollierung/Alarmierung/Nachvollziehbarkeit, Notfallreaktion, Datenschutz/Arbeitsrecht/Compliance, Anbieter/Updates/Lieferkette, speziell Fernwartung durch externe Dienstleister auf Ihren Systemen (Fall B), speziell Betrieb für mehrere Kunden (Fall C, Dienstleister/MSP) sowie organisatorische Grundlagen in Ihrem Unternehmen. Jede Anforderung ist mit Anforderung, Gründen und Prüfanleitung ("So wird geprüft") versehen. Dort finden sich außerdem die Prioritäten (MUSS/SOLL/KANN), das Bewertungsschema (0–3 Punkte je Anforderung) und die Entscheidungsregel für die Auswahl.
- **Langfassung 09:** Enthält zusätzlich die Belegstellen und Zitate je Anforderung, die Ausschreibungshilfen (Abschnitt 4.3 der Langfassung) sowie die Entscheidungshilfe zu Betriebsmodellen und Anbieter-Warnsignalen (Kapitel 6 der Langfassung).

5. Quellen und Herleitung

Jede Anforderung stammt aus einer von drei Quellgruppen: (1) dem *Fern-Compass-Framework* mit Expertentipps als technische Detailbegründung nebst Prüfanleitungen, (2) der Interview-Spezifikation mit Unternehmen des technischen Service sowie (3) Normen und Regulierung: BSI IT-Grundschutz (u. a. OPS.1.2.5 "Fernwartung"), NIS2/BSIG (§ 30/32), DSGVO, BetrVG, ISO/IEC 27001:2022, CIS Controls v8, NIST SP 800-53 sowie die CRA (Verordnung (EU) 2024/2847) und die zugehörige BSI-TR-03183.

6. Glossar

Begriff	Bedeutung
Agent	Kleines Programm auf jedem gewarteten Gerät; hält die Verbindung zur Verwaltungskonsole und führt Aktionen aus.
Verwaltungskonsole	Die zentrale Oberfläche, über die Sitzungen gestartet, Rechte und Geräte überwacht werden.
Vermittlungsdienst (Relay)	Server, über den sich Konsole und Agent treffen, ohne dass eingehende Ports auf den Geräten geöffnet werden müssten.
MFA	Multifaktor-Authentisierung: Anmeldung mit zwei unabhängigen Beweisen.
FIDO2 / Passkey	Anmeldestandards mit kryptografischem, gerätegebundenem Nachweis.
TLS	Transport Layer Security: Standardprotokoll zur Verschlüsselung von Verbindungen.
Ende-zu-Ende-Verschlüsselung (E2E)	Nur die Endpunkte (Techniker-Gerät, Zielgerät) können die Sitzung entschlüsseln; der Vermittlungsserver sieht nur Chiffre.
SBOM	Software Bill of Materials, die Liste aller in einem Produkt enthaltenen Komponenten.
Notfall-Abschalter	Verfahren, die Fernwartung flächendeckend stillzulegen.
OT	Operational Technology, also Steuerungs-/Produktionstechnik (SPS, Maschinensteuerung) im Unterschied zur klassischen IT.
SaaS	Software-as-a-Service, ein Abo-Modell für Ready-to-Use Software in der Cloud.
AVV	Auftragsverarbeitungsvertrag nach Art. 28 DSGVO.
Zero-Trust	Sicherheitsansatz, bei dem kein Zugriff a priori vertraut wird; jeder Zugang muss geprüft werden.
MSP	Managed Service Provider: externer IT-Dienstleister, der Systeme betreibt (Fall C).
RMM	Remote Monitoring and Management: Software zur Fernverwaltung ganzer Geräteflotten.

7. Förderhinweis

FERN-KOMPASS gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren und der Initiative IT-Sicherheit in der Wirtschaft umfassende Unterstützung bei der Digitalisierung mit dem Schwerpunkt Künstliche Intelligenz. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung. Weitere Informationen finden Sie unter www.mittelstand-digital.de.