



FERN-KOMPASS
Sichere Fernwartung
für KMU

Anforderungscheckliste »Sichere Fernwartung« für KMU

Erweitert

Gefördert durch:



Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital



aufgrund eines Beschlusses
des Deutschen Bundestages

www.fern-kompass.de · Stand: September 2026

Inhalt

1. Wofür Sie diese Checkliste brauchen.....	3
2. Warum Fernwartung besonders gut geschützt sein muss	3
3. Schnellprüfung: Zehn Fragen, die jede Lösung bestehen muss	5
4. Prioritäten und Bewertung.....	6
4.1 Prioritäten	6
4.2 Bewertung und Entscheidungsregel	6
5. Die Checkliste im Detail	7
5.1 Identität und Zugriff: Wer darf fernwarten, und wie sicher ist der Schlüssel?	7
5.2 Sitzungssicherheit: Freigabe, Verschlüsselung, Aufzeichnung	9
5.3 Agent und Endgeräte: Was auf Ihren Systemen läuft	11
5.4 Netzwerk-Anbindung und Infrastruktur: Wie alles angebunden ist	14
5.5 Protokollierung, Alarmierung, Nachvollziehbarkeit	15
5.6 Notfallreaktion: Wenn es trotzdem passiert.....	17
5.7 Datenschutz, Arbeitsrecht und Compliance	18
5.8 Anbieter, Updates und Lieferkette: Wem Sie vertrauen	19
5.9 Speziell: Fernwartung durch externe Dienstleister auf Ihren Systemen (Fall B)	21
5.10 Speziell: Betrieb für mehrere Kunden (Dienstleister/MSP, Fall C).....	23
5.11 Organisatorische Grundlagen in Ihrem Unternehmen: Auch die beste Lösung reicht nicht allein.....	23
6. Quellen und Herleitung	25
7. Glossar	25
8. Förderhinweis	26

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:

- Neubeschaffung:** Arbeiten Sie Abschnitt 3 (Schnellprüfung) und dann Abschnitt 5 vollständig durch.
- Bestandslösung bewerten:** Prüfen Sie zuerst die K.O.-Kriterien aus Abschnitt 3. Besteht Ihre Lösung sie nicht, haben Sie Handlungsbedarf, unabhängig von allem anderen.
- Dienstleister-Zugriffe auf Ihre Maschinen:** Wenn nicht Sie fernwarten, sondern ein Hersteller oder Dienstleister auf Ihre Anlagen zugreift, ist Abschnitt 5.9 Ihr Kernkapitel.

Welcher Fall betrifft Sie?

Fall	Ihre Situation	Relevante Kapitel
A	Sie fernwarten Ihre eigenen Geräte (IT-Support, Server, Arbeitsplätze)	5.1–5.8, 5.11
B	Externe (Maschinenhersteller, Dienstleister) fernwarten Ihre Maschinen/Anlagen	5.9, 5.2, 5.5, 5.7, 5.11
C	Sie sind selbst Dienstleister und fernwarten Systeme Ihrer Kunden	alle, zusätzlich 5.10

Die Fälle schließen sich nicht aus; auf 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:

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

Vorfall	Was passierte	Die Lücke, die es ausnutzte
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) kompromittierten 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 Abrechnungsoftware-Anbieters und kompromittierten 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 in dieser Checkliste überwiegend verhindern, begrenzen oder zumindest bemerken. Jede Anforderung ist einem dieser realen Schadensmuster oder einer gesetzlichen Pflicht zugeordnet. Das begründet sie, macht sie aber nicht in jedem Einzelfall unverzichtbar.

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 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: Die Schwachstellen- und Vorfallmeldepflichten 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 prüfen vor dem Detailvergleich die MUSS-Anforderungen und müssen alle zufriedenstellend beantwortet werden. Die zugehörigen Detailanforderungen stehen in Klammern.

#	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 gestohlenen Passwort allein keinen Zugang ermöglicht. (CL-IAA-01)
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. (CL-SES-01)
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. (CL-AGT-01)
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. (CL-LOG-01, CL-LOG-04)
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. (CL-SES-02)
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. (CL-NET-01)
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. (CL-NET-02)
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. (CL-IR-01, CL-IR-02)
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. (CL-GOV-03, CL-GOV-04)
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. (CL-IAA-02)

4. Prioritäten und Bewertung

4.1 Prioritäten

Priorität	Bedeutung	Konsequenz bei Nichterfüllung
MUSS	Zwingend erforderlich. Entspricht überwiegend der Stufe P0 des Fern-Compass-Frameworks; die Zuordnung kann im Einzelfall abweichen, weil Checklisten-Positionen mehrere SR-Anforderungen zusammenfassen oder aufteilen.	Lösung scheidet aus bzw. muss nachgerüstet werden, bevor sie produktiv geht.
SOLL	Dringend empfohlen; standardmäßig aktivieren. Entspricht P1. Reduziert das Restrisiko deutlich bei überschaubarem Aufwand.	Abweichung nur mit dokumentierter Risikoakzeptanz durch die Geschäftsführung.
KANN	Sinnvoll, wo die Lösung es hergibt. Entspricht P2 (Vertiefung/Reifegrad).	Keine; als Roadmap-Thema notieren.

Einige MUSS-Anforderungen sind zusätzlich als **K.O.** markiert: Sie disqualifizieren eine Lösung bereits in der Vorprüfung (vgl. Abschnitt 3).

4.2 Bewertung und Entscheidungsregel

Bewerten Sie jede Anforderung mit 0–3 Punkten:

Punkte	Bedeutung
0	Nicht erfüllt, keine Roadmap
1	Teilweise erfüllt oder nur mit erheblichem Eigenaufwand
2	Erfüllt nach Konfiguration
3	Erfüllt ab Werk / in der Standardeinstellung, sofern die Voreinstellung sicher ist. Standardmäßig aktivierte Aufzeichnungs- oder Überwachungsfunktionen sind keine sichere Voreinstellung und begründen keine Höchstwertung.

Entscheidungsregel:

1. Alle K.O.-Kriterien bestanden? Sonst: ausscheiden.
2. Alle MUSS-Anforderungen mit mindestens 2 Punkten? Sonst: ausscheiden oder Nachrüstung zur Bedingung machen.
3. Vergleich mehrerer geeigneter Kandidaten anhand der Summe über MUSS + SOLL (Gewichtungsvorschlag: MUSS zählt doppelt).

Bewahren Sie das ausgefüllte Exemplar auf; es dient später als Nachweis der sorgfältigen Auswahl (auch relevant für NIS2-Dokumentationspflichten und Versicherungsfragen).

5. Die Checkliste im Detail

5.1 Identität und Zugriff: Wer darf fernwarten, und wie sicher ist der Schlüssel?

Der häufigste Weg in ein Fernwartungssystem ist kein Software-Fehler, sondern ein gestohlener oder wiederverwendeter Zugang. Alles in diesem Abschnitt dreht sich darum, dass nur die richtigen Personen mit gut gesicherten Schlüsseln hineinkommen und dass ein einmal geklauter Schlüssel möglichst wenig öffnet. Gleichzeitig werden mit diesen Punkten die Gefahr durch Phishing minimiert.

CL-IAA-01 · Multifaktor-Authentisierung (MFA) für jeden Zugang

MUSS · K.O. ☐

Anforderung: Für interaktive menschliche Anmeldungen an der Verwaltungskonsole (auch für "nur lesende" Konten) gilt: kein Zugang mit Passwort allein; bevorzugt phishing-resistente, passwortlose Verfahren (FIDO2-Sicherheitsschlüssel, Passkeys), sonst MFA mit zweitem, unabhängigem Faktor. Ein reines Passwort-Login darf nicht existieren oder muss sich abschalten lassen. Für nicht-interaktive technische Identitäten (Agenten-, Dienst- und Maschinenkonten) gelten andere Regeln: keine interaktiven Passwort-Anmeldungen, sondern pro Gerät ausgegebene Zertifikate oder kurzlebige Maschinen-Credentials. Für Administratoren bevorzugen Sie phishing-resistente Verfahren (FIDO2-Sicherheitsschlüssel, Passkeys); TOTP-App oder Push-Verfahren genügen nur für niedrig privilegierte Rollen.

Gründe: Account-Übernahmen durch Passwortdiebstahl und -wiederverwendung sind der klassische Einstieg. Ein zweiter Faktor stoppt genau diese Angriffe. Die EU-Durchführungsverordnung 2024/2690 bezeichnet phishing-resistente MFA als Stand der Technik für risikoreiche Zugriffe; SMS-Codes gelten dafür als überholt.

So wird geprüft: Prüfen Sie beides getrennt: (1) Interaktive Anmeldung: Versuch mit korrektem Passwort ohne zweiten Faktor muss scheitern. (2) Technische Identitäten: Agent-/Dienstkonten authentifizieren sich nicht-interaktiv über gerätebezogene Zertifikate oder kurzlebige Credentials, nicht über Passwort + zweitem Faktor.

CL-IAA-02 · Rollen und gerätebezogene Rechte

MUSS ☐

Anforderung: Rechte werden nach Rollen (z. B. Betrachter, Techniker, Senior-Techniker, Administrator) und bezogen auf bestimmte Geräte oder Gerätegruppen vergeben. Ein Techniker-Konto kann nur auf die ihm zugewiesenen Geräte zugreifen; Zugriffsversuche darüber hinaus werden verweigert und protokolliert. Administrative Rollen sind von normalen Benutzerrollen getrennt.

Gründe: Begrenzte Rechte begrenzen den Schaden. Wenn ein Techniker-Konto kompromittiert wird, betrifft es "nur" die zugewiesenen Geräte, nicht die gesamte Geräteflotte. Genau diese Begrenzung fehlte beim Kaseya-Vorfall, wo ein einziges kompromittiertes System zur flächendeckenden Erpressungssoftware-Verteilung reichte.

So wird geprüft: Lassen Sie in einer Teststellung mit einem Techniker-Konto eine Sitzung zu einem nicht zugewiesenen Gerät öffnen; sie muss abgelehnt und als Ereignis protokolliert werden.

CL-IAA-03 · Anbindung an zentrales Identitätsmanagement (SSO)

MUSS ☐

Anforderung: Die Konsole lässt sich an Ihr zentrales Identitätsverfahren (Single Sign-On über OIDC oder SAML) anbinden. Lokale Konten existieren nur als dokumentierte Ausnahmen. Verlässt ein Mitarbeitender das Unternehmen, entfällt der Zugang automatisch mit der Deaktivierung im Identitätsdienst.

Gründe: Ohne zentrale Anbindung entstehen Schattenkonten, die niemand löscht und die bei Ausscheiden von Mitarbeitenden oder Dienstleistern einfach weiterbestehen. Die Interview-Analyse zeigt hier eine Prioritätsverfehlung der Quelle (MFA/SSO nur "Soll"): Aus heutiger Sicherheits- und NIS2-Sicht sind SSO und MFA Muss. NIS2 fordert starke Authentisierung und Cyber-Hygiene, ohne SSO ausdrücklich vorzuschreiben.

So wird geprüft: Deaktivieren Sie einen Testbenutzer im Identitätsdienst; der Zugang zur Konsole muss sofort enden.

CL-IAA-04 · Notfallkonten (Break-Glass) geregelt

MUSS ☐

Anforderung: Für den Ausfall des Identitätsdienstes existieren ein bis zwei dokumentierte Notfallkonten. Sie sind mit phishing-resistenten Faktoren (Hardware-Schlüssel, Zertifikat) gesichert, dürfen im Tagesgeschäft nicht verwendet werden, und jede Nutzung löst einen Alarm aus.

Gründe: Wenn der Identitätsdienst ausgefallen ist, dürfen Sie weder ausgesperrt sein noch sich mit einem schwachen Hintertür-Konto einladen. Nicht dokumentierte, schwach gesicherte Notfallkonten sind erfahrungsgemäß die am längsten unentdeckte Schwachstelle. Zudem gilt: **Keine Standard- oder Werkskennwörter**; Angriffe über unveränderte Admin-Passwörter sind vielfach belegt.

So wird geprüft: Prüfen Sie die Dokumentation und führen Sie den Notfall-Zugang einmal im Test aus: Anmeldung, Protokollierung und Alarm müssen nachweisbar funktionieren.

CL-IAA-05 · Zeitlich begrenzte Rechte (Just-in-Time) statt Dauerverwaltung

MUSS ☐

Anforderung: Erweiterte Rechte (z. B. Zugriff auf Produktionsserver, Ausführung privilegierter Aktionen) werden auf Zeit vergeben und laufen automatisch ab; Dauerverwaltungsrechte sind die dokumentierte Ausnahme, nicht die Regel. Die Freigabe kann risikobasiert erfolgen: für Produktionssysteme als Approval-Workflow (zweite Person oder Ticket), für weniger kritische Systeme automatisch dokumentiert.

Gründe: Stehende Administrationsrechte sind der wertvollste Beutezug für einen Angreifer und der Hebel, über den beim Kaseya-Vorfall aus einem einzigen kompromittierten Konto eine flächendeckende Attacke wurde. Zeitlich begrenzte, freigegebene Rechte verkleinern das Zeitfenster und die Angriffsfläche dramatisch.

So wird geprüft: Beantragen Sie eine Rechte-Erhöhung, lassen Sie sie ablaufen und versuchen Sie die Aktion erneut; sie muss verweigert werden.

CL-IAA-06 · Bedingter Zugriff

SOLL ☐

Anforderung: Der Zugang zur Konsole kann an Bedingungen geknüpft werden: Quelle (IP-Bereich, Land), verwaltetes Gerät, Uhrzeit. Zugriffe außerhalb der Regel werden abgewiesen oder erfordern eine zusätzliche Bestätigung.

Gründe: Selbst mit MFA gilt: Je enger der legitime Zugangsweg, desto auffälliger jeder andere. Eine Anmeldung aus einem unerwarteten Land um 3 Uhr nachts ist ein Warnsignal, dem Sie nachgehen sollten; bedingter Zugriff kann solche Zugriffe abweisen oder an zusätzliche Bestätigung binden. Ein kategorisches Länder-Blocking ist nur dann richtig, wenn es Ihre Risiko- und Nutzungslage (z. B. legitime Remote-Zugriffe auf Reisen) verlangt.

So wird geprüft: Versuchen Sie in der Teststellung den Zugang von einem nicht verwalteten Gerät bzw. außerhalb der freigegebenen Zeiten.

5.2 Sitzungssicherheit: Freigabe, Verschlüsselung, Aufzeichnung

Eine Fernwartungssitzung überträgt alles, was auf dem Bildschirm passiert: Dateiinhalte, Zugangsdaten, die gerade getippt werden, geschäftskritische Abläufe. Dieser Abschnitt stellt sicher, dass eine Sitzung nur mit Wissen der Betroffenen, verschlüsselt und nachvollziehbar stattfindet.

CL-SES-01 · Durchgängige Verschlüsselung aller Verbindungen

MUSS · K.O. ☐

Anforderung: Sämtlicher Verkehr, also Anmeldung an der Konsole, Sitzungsdaten (Bildschirm, Tastatur, Dateien) und Agent-Kommunikation, ist mit TLS 1.2, TLS 1.3 oder vergleichbaren Verfahren unter Verwendung moderner Chiffren geschützt. Bei ungültigen oder abgelaufenen Zertifikaten bricht die Verbindung kontrolliert ab ("fail closed"); ein unverschlüsselter Rückfall existiert nicht.

Gründe: Der Inhalt einer Fernwartungssitzung ist Beute: Passwörter, Kunden- und Geschäftsdaten, Maschinenparameter. Unverschlüsselte oder schwach verschlüsselte Verbindungen lassen sich in offenen Netzen (Hotel, Messe, Kunden-Standort) oder auf dem Übertragungsweg mitlesen. Verschlüsselung ist zugleich Grundanforderung aus DSGVO und NIS2.

So wird geprüft: Lassen Sie die Konsole und den Server-Dienst mit einem frei verfügbaren Prüftool (z. B. `testssl.sh`) auf veraltete Verfahren testen.

CL-SES-02 · Aktive Freigabe, sichtbarer Hinweis und lokaler Stopp am Zielgerät

MUSS · K.O. ☐

Anforderung: Auf Geräten von Mitarbeitenden beginnt eine betreute Sitzung erst nach ausdrücklicher, vorheriger Freigabe durch die betroffene Person (bzw. den Betreiber); eine bloße Ankündigung ist keine gleichwertige Alternative. Ein Banner zeigt wer sich verbindet (Name des Technikers, Firma) und warum (Anlass/Ticket), inkl. Kontaktmöglichkeit. Die Person am Gerät kann die Sitzung jederzeit lokal beenden. Unbeaufsichtigte Sitzungen sind nur als separat konfigurierte, bereichsabgegrenzte, zeitlich befristete, stark authentifizierte und überwachte Ausnahme zulässig.

Gründe: Das schützt in drei Richtungen: die betroffenen Mitarbeitenden (Transparenz ist Voraussetzung für Datenschutz und Mitbestimmung, § 87 Abs. 1 Nr. 6 BetrVG), Ihr Unternehmen gegen Innentäter (wer weiß, dass Name und Anlass aufgezeichnet werden, verhält sich

regelkonform) und gegen Betrugsanrufe (die betroffene Person sieht, dass und wer verbunden ist und kann den "Techniker" beenden, der sich per Anruf hereingedrückt hat). Die interviewten Unternehmen bewerteten genau diese aktive Freigabe als Kernfunktion; die Interview-Quelle nimmt sie ausdrücklich in ihre CRA-Paraphrase auf (ER.5: "Freigabe und Kontrolle jeder Fernwartungssitzung", eine projektinterne Interview-Erweiterung, kein amtlicher CRA-Wortlaut). Die amtliche CRA fordert allgemeiner geeignete Kontrollmechanismen gegen unbefugten Zugriff (Anhang I Teil I Nr. 2 Buchst. d).

So wird geprüft: Starten Sie in der Teststellung eine betreute Sitzung auf einem Testgerät mit Mitarbeitenden-Konto: Ohne vorherige Freigabe darf keine Verbindung entstehen; Banner mit Identität und Anlass sichtbar; Beenden-Schaltfläche wirksam?

CL-SES-03 · Ende-zu-Ende-Verschlüsselung der Sitzungen

SOLL ☐

Anforderung: Sitzungen werden ende-zu-ende verschlüsselt: Der Vermittlungsserver kann den Sitzungsinhalt nicht entschlüsseln; jede Sitzung verwendet eigene, kurzlebige Schlüssel. Der Anbieter muss die Verschlüsselungsarchitektur dokumentiert beschreiben (Schlüsselvergabe, was der Server sehen kann).

Gründe: Ohne Ende-zu-Ende-Verschlüsselung endet die Vertraulichkeit am Server des Anbieters bzw. Ihres Vermittlungsservers: Wer diesen Server kompromittiert, kann künftig alle Sitzungen mitlesen. Achtung bei Marketingaussagen: Ende-zu-Ende-Verschlüsselung ist seltener, als Werbung vermuten lässt; viele Produkte entschlüsseln am Server.

Akzeptable Alternative: Der Vermittlungsdienst läuft auf einem von Ihnen betriebenen, gehärteten und überwachten Server, und Sitzungen werden aufgezeichnet; dann ist die Transparenz beim Betreiber wenigstens kontrollierbar.

So wird geprüft: Fordern Sie die Dokumentation der Verschlüsselungsarchitektur an. Verlangen sie eine formelle Dokumentation, keine Werbematerialien.

CL-SES-04 · Sitzungsmetadaten vollständig erfasst

MUSS ☐

Anforderung: Für jede Sitzung werden automatisch erfasst: Beginn und Ende, initiiierende Person, Zielgerät, Quell-Adresse und Anlass-/Ticket-Bezug. Die Daten bleiben über den vereinbarten Zeitraum abrufbar.

Gründe: Ohne diese Metadaten können Sie im Ernstfall weder nachvollziehen, wer wann wo war, noch eine Abweichung bemerken (Sitzung auf einem Produktionsserver um Mitternacht?). Sie sind zugleich die Grundlage für jede Meldung nach NIS2/DSGVO und für die Abgrenzung gegenüber Dienstleistern.

So wird geprüft: Führen Sie eine Sitzung durch und prüfen Sie den erzeugten Protokolleintrag auf Vollständigkeit.

CL-SES-05 · Sitzungslimits (Leerlauf und Höchstdauer)

SOLL ☐

Anforderung: Die Lösung erzwingt konfigurierbare Limits: automatischer Verbindungsabbruch bei Leerlauf (z. B. 10 Minuten) und eine maximale Sitzungsdauer pro Rolle/Gerätekategorie.

Gründe: Vergessene, offene Sitzungen sind ein unterschätztes Risiko; ein hängen gebliebenes Fenster ist ein offenes Fenster. Im industriellen Umfeld ist eine maximale Sitzungsdauer zugleich BSI-Anforderung.

So wird geprüft: Leerlauf-Sitzung laufen lassen: sie muss automatisch trennen.

CL-SES-06 · Dateiübertragung und Zwischenablage geregelt

SOLL ☐

Anforderung: Dateiübertragung und Zwischenablage-Freigabe sind standardmäßig deaktiviert und werden pro Rolle/Gerätegruppe policy-basiert freigegeben. Jede Übertragung wird protokolliert (Dateiname, Größe, Richtung, Prüfsumme).

Gründe: Die Übertragungsfunktion ist der praktischste Weg für Datenabfluss (Innentäter, kompromittierter Techniker) wie für das Einschleusen von Schadsoftware. "Aus, außer wenn ausdrücklich erlaubt und jede Bewegung protokolliert" dreht das Verhältnis um.

So wird geprüft: Versuchen Sie in der Standardkonfiguration eine Dateiübertragung. Sie muss scheitern; nach Freigabe muss ein Protokolleintrag entstehen.

CL-SES-07 · Aufzeichnung privilegierter Sitzungen, manipulationssicher

SOLL ☐

Anforderung: Sitzungen mit erweiterten Rechten (Server, Produktion, sensible Systeme) können aufgezeichnet werden. Die Aufzeichnungen sind manipulationssicher gespeichert (nur-anhängbar oder kryptografische Verkettung) und werden nach festgelegter Frist automatisch gelöscht.

Gründe: Aufzeichnungen sind Ihr Beweismittel im Ernstfall: gegen Innentäter, gegen Fehlbedienungsvorwürfe, für Versicherungen und Behörden. Manipulationssicherheit ist der Kern: Eine Aufzeichnung, die der aufgezeichnete Administrator selbst ändern könnte, ist vor Angreifern und vor Gericht wertlos. **Wichtig:** Vor der Aktivierung von Aufzeichnung auf Mitarbeiter-PCs zwingend Abschnitt 5.11 (Betriebsvereinbarung) beachten.

So wird geprüft: Versuchen Sie in der Teststellung als lokaler Administrator, eine Aufzeichnung zu ändern oder zu löschen; es muss scheitern und Alarm auslösen.

5.3 Agent und Endgeräte: Was auf Ihren Systemen läuft

Der Agent ist das kleine Programm, das auf jedem gewarteten Gerät installiert wird und die Verbindung zur Konsole hält. Er läuft oft mit höchsten Rechten; deshalb ist seine Integrität der heikelste Punkt der ganzen Lösung: Ein manipulierter oder gefälschter Agent ist eine dauerhafte Hintertür.

CL-AGT-01 · Signierter Agent mit Integritätsprüfung

MUSS · K.O. ☐

Anforderung: Agent-Programme und Installation-Pakete sind vom Hersteller digital signiert; die Installation prüft die Signatur. Der Agent verifiziert beim Start seine eigene Datei- und Konfigurationsintegrität und meldet Manipulationen an die Verwaltungsebene.

Gründe: Unsignierte oder ungeschützte Agenten lassen sich durch Schadsoftware ersetzen oder patchen; der "Wächter" wird selbst zur Hintertür. Der AnyDesk-Vorfall (gestohlene Signaturzertifikate) zeigt, wie wertvoll Signaturen sind: Angreifer investieren erheblich, um sie zu bekommen. Zugleich zeigt der Fall die Grenzen: Signaturen belegen Herkunft und Integrität, stoppen aber keine korrekt signierte, bösartige Ausgabe nach Build-/Signatur-Kompromittierung. Verlangt auch die CRA (sichere Verbreitung von Aktualisierungen, Integritätsschutz).

So wird geprüft: Prüfen Sie die Signatur der Agenten-Datei auf einem Testgerät mit Bordmitteln; in einer vom Anbieter freigegebenen, isolierten Testumgebung dürfen Sie ein Byte ändern und neu

starten; der Agent muss die Manipulation melden. Ohne solche Umgebung: Anbieter-Erklärung oder unabhängige Prüfung als Beleg heranziehen.

CL-AGT-02 · Gegenseitige Authentifizierung zwischen Agent und Server

MUSS ☐

Anforderung: Agent und Vermittlungsserver authentifizieren sich gegenseitig (z. B. mTLS mit gerätespezifischen Zertifikaten oder gerätespezifischen Token). Der Agent akzeptiert nur den ihm zugewiesenen Server ("Pinning"); ein fremder Server mit selbstsigniertem Zertifikat wird abgewiesen.

Gründe: Ohne gegenseitige Authentifizierung kann sich (a) ein fremder Agent als Ihres ausgeben, um "Insider-Zugang" zu Ihrem Bestand zu erhalten, oder (b) ein gefälschter Server zwischen die Verbindung schalten. Beides sind dokumentierte Angriffsmuster.

So wird geprüft: Entfernen Sie das Client-Zertifikat eines Test-Agenten und richten Sie ihn auf einen Server mit selbstsigniertem Zertifikat; beide Verbindungen müssen kontrolliert scheitern.

CL-AGT-03 · Geschützte Deinstallation mit Alarm

MUSS ☐

Anforderung: Der Agent lässt sich nur mit einem Geheimnis bzw. über eine Richtlinien-Freigabe deinstallieren oder deaktivieren, das ein lokaler Benutzer nicht beschaffen kann. Versuchte Deinstallationen durch lokale Administratoren und erfolgreiche Deinstallationen lösen Alarm aus.

Gründe: Der erste Schritt eines Angreifers auf einem kompromittierten Gerät ist regelmäßig, den Wächter zu entfernen. Erfolgt das still, verlieren Sie die Sicht; mit Alarm wird daraus ein früh erkennbares Warnsignal.

So wird geprüft: Versuchen Sie auf einem Testgerät die Deinstallation als lokaler Administrator ohne Geheimnis; sie muss scheitern und alarmieren.

CL-AGT-04 · Signierte, gestuft ausgerollte Updates

MUSS ☐

Anforderung: Agenten-Updates werden über einen festgelegten Kanal mit signierten Update-Paketen verteilt. Der Rollout erfolgt gestuft: eine kleine Pilotgruppe ("Canary") zuerst, die Flotte erst nach einer Bewährungsphase. Ein dokumentiertes Rollback-Verfahren existiert.

Gründe: Der Update-Kanal ist der mächtigste Hebel der Lieferkette: Beim Kaseya-Vorfall wurde die Erpressungssoftware über den regulären, vertrauenswürdigen Verteilweg des Herstellers selbst ausgeliefert; SolarWinds zeigte dasselbe Muster. Signierte Pakete verhindern die Annahme unsignierter oder nicht autorisierter Update-Pakete und belegen Herkunft und Integrität; gestufter Rollout verhindert, dass ein fehlerhaftes oder kompromittiertes Update sofort alle Geräte trifft. Signaturen schützen allerdings nicht vor einem korrekt signierten, bösartigen Update nach Kompromittierung des Build- oder Signaturprozesses; deshalb bleiben Canary-Gruppen, dokumentiertes Rollback und unabhängige Release-Kontrollen unverzichtbar.

So wird geprüft: In einer vom Anbieter freigegebenen, isolierten Teststellung: ein korrekt signiertes Test-Update veröffentlichen (nur Pilotgruppe erhält es) und ein falsch signiertes (muss flächendeckend abgelehnt werden). Ohne solche Umgebung: Anbieter-Erklärung oder unabhängige Prüfung als Beleg heranziehen.

CL-AGT-05 · Minimale Rechte des Agenten

SOLL ☐

Anforderung: Der Agent läuft mit möglichst geringen Rechten. Erweiterte Ausführung (als SYSTEM/root) erfolgt nur für die Dauer einer konkreten, autorisierten Aktion.

Gründe: Ein Agent, der dauerhaft mit Höchstrechten läuft, verwandelt jede Kompromittierung der Konsole in vollständige Gerätekontrolle, das genaue Muster der Kaseya-Attacke. Minimale Rechte brechen diesen Domino-Effekt.

So wird geprüft: Frage an den Anbieter: "Mit welchen Rechten läuft der Agent im Grundzustand, und wie wird die Rechte-Erhöhung pro Aktion kontrolliert?".

CL-AGT-06 · Geschützte Skriptausführung und begrenzte Massenaktionen

SOLL ☐

Anforderung: Die Ausführung von Skripten/Befehlen auf Geräten unterstützt spezielle Freigabe-Workflows für risikoreiche Operationen und ein Repository signierter bzw. per Prüfsumme fixierter Skripte. Massenaktionen (Skriptausführung auf viele Geräte gleichzeitig) sind freigabepflichtig, begrenzt und lösen oberhalb definierter Schwellen einen Alarm aus.

Gründe: Die Funktionen "Skript auf alle Endgeräte ausführen" dient als Verbreitung von Ransomware, die Kaseya-Attacke lief exakt so ab. Durch die Einrichtung von Freigaben, Limits und Alarmen wird ein kontrollierter Ablauf bei Massenausführungen sichergestellt.

So wird geprüft: Erkundigen Sie sich nach den Konfigurationsmöglichkeiten für Freigabe-Workflows und Massenaktions-Schwellen. Zudem sollte geprüft werden, ob eine Massenausführung ohne Freigabe möglich ist.

CL-AGT-07 · Agent-Gesundheit überwacht, Telemetrie weiterleitbar

SOLL ☐

Anforderung: Der Agent-Zustand wird überwacht: ein über eine Schwelle hinaus "stiller" Agent, eine Deinstallation oder wiederholte fehlgeschlagene Verbindungsversuche erzeugen einen Alarm. Ein stiller Agent gilt als mögliches Manipulationsereignis. Sicherheitsrelevante Ereignisse am Endgerät (Prozesse, Netzwerkverbindungen, Anmeldungen) können an die Verwaltungsebene oder ein Auswertungssystem (SIEM) weitergeleitet werden.

Gründe: Ein still verschwundener Agent ist ein Warnsignal, dem nachgegangen werden muss: Es kann eine Abschaltung durch einen Angreifer sein, aber auch einen harmloseren Grund haben, beides verlangt eine Nachverfolgung.

So wird geprüft: Stoppen Sie den Agent-Dienst auf einem Testgerät und deinstallieren Sie ihn auf einem anderen Testgerät. Beides muss als potentielle Manipulation zu einem Alarm führen.

CL-AGT-08 · Getestete Plattform-Abdeckung mit Sicherheits-Mindestniveau

MUSS ☐

Anforderung: Die unterstützten Betriebssysteme und Versionen sind in einer Kompatibilitätsmatrix dokumentiert und vom Hersteller getestet, ausdrücklich einschließlich älterer, im Feld noch eingesetzter Windows-Versionen. Für Altsysteme ist ein Sicherheits-Mindestniveau definiert (z. B. TLS-1.2-Fähigkeit, laufender Sicherheits-Support des OS); Systeme darunter werden nicht angeschlossen, sondern isoliert betreut.

Gründe: Die interviewten Unternehmen betreiben bewusst Alt-Windows neben aktuellen Systemen. Aber: Alte Systeme ohne Sicherheits-Funktionen (moderne Verschlüsselung, Signaturprüfung) untergraben jede andere Anforderung dieser Liste. Ohne definiertes Mindestniveau kollidieren "Alt unterstützen" und "sicher sein" frontal, deshalb gehört die Grenze vor dem Anschluss festgelegt.

So wird geprüft: Fordern Sie die Kompatibilitätsmatrix inkl. Testnachweis an. Gleichen Sie Ihre Alt-Systeme dagegen ab und legen Sie das Mindestniveau schriftlich fest.

5.4 Netzwerk-Anbindung und Infrastruktur: Wie alles angebunden ist

Die Angriffswellen der letzten Jahre hatten ein gemeinsames Vorspiel: eine frei aus dem Internet erreichbare Verwaltungsoberfläche. KI-Agenten, die automatisch neue Softwareversionen auf Sicherheitspatches analysieren haben die Zeit zwischen öffentlich-werden und dem Ausnutzen von Schwachstellen rapide verkürzt. Dieser Abschnitt stellt sicher, dass Ihre Fernwartungs-Infrastruktur von außen weder sichtbar noch erreichbar ist und im Innenleben Ihres Netzes eine eigene, abgetrennte Rolle spielt.

CL-NET-01 · Agenten verbinden sich nur ausgehend

MUSS · K.O. ☐

Anforderung: Die Agenten bauen nur ausgehende Verbindungen auf. Auf den gewarteten Geräten sind keine eingehenden Firewall-Freigaben nötig.

Gründe: Jede eingehende Freigabe ist ein Loch, das von außen gefunden und ausgenutzt werden kann; das ist der Grund, warum der Rendezvous-Ansatz in vielen Bereichen zum Standard wurde. Für industrielle Umgebungen ist "nur ausgehend" eine Kern-Anforderung des BSI. Zugleich vereinfacht es das Firewall-Management beim Betreiber erheblich. Dieser Punkt allein ist notwendig, aber nicht hinreichend: Der Kanal muss zusätzlich zielbeschränkt sein (fest definierte Ziele/Ports) und gegenseitig authentisiert werden.

So wird geprüft: Prüfen Sie auf einem Testgerät die Firewall-Regeln: keine eingehenden Regeln für den Agent -> die Verbindung funktioniert trotzdem.

CL-NET-02 · Verwaltungskonsole nicht anonym aus dem Internet erreichbar

MUSS · K.O. ☐

Anforderung: Die gesamte Verwaltungsebene, einschließlich API, ist nicht direkt und unauthentifiziert aus dem Internet abrufbar. Der Zugang erfolgt nur über VPN, IP-Freigabeliste oder eine vorgeschaltete Identitäts-/Zero-Trust-Schicht.

Gründe: Das ist der wichtigste Einzel-Schutz dieses Dokuments: Mehrere vergangene Attacken begannen mit öffentlich erreichbaren Verwaltungsflächen. Nicht-Exposition verkleinert diese Angriffsklasse beträchtlich, ist aber keine Immunisierung: verbleibende Schwachstellen der Zugangsschicht bleiben erreichbar.

So wird geprüft: Rufen Sie von einem externen Anschluss (z. B. Mobilfunk) die Konsolen-Adresse ohne Anmeldung ab. Sie müssen an einer Authentifizierungs-/Zugangsschicht abgewiesen werden.

CL-NET-03 · Fernwartungs-Infrastruktur netzlich getrennt

MUSS beim Selbstbetrieb / SOLL bei SaaS ☐

Anforderung: Beim Selbstbetrieb leben Konsole, Vermittlungsdienst und Datenbank in einem eigenen, abgetrennten Netzsegment (Verwaltungs-/DMZ-Segment) mit minimalen, dokumentierten Freigaben zu den übrigen Netzen. Bei SaaS/Cloud fragen Sie den Anbieter nach der Umgebungs- und Mandantentrennung seiner Plattform.

Gründe: Die Verwaltungsebene ist eine Höchst-Privileg-Anlage: Wer sie einmal kontrolliert, kontrolliert alle Geräte. Eine Trennung begrenzt den Explosionsradius und funktioniert nachweislich: Beim TeamViewer-Einbruch 2024 blieben Produktdaten verschont, gerade weil der Hersteller interne Umgebungen getrennt hatte.

So wird geprüft: Beim Selbstbetrieb: port-scan des Verwaltungssegments aus dem Büro-Netz. Nur dokumentierte Ports dürfen antworten. Bei SaaS und Cloud: Frage an die jeweiligen Anbieter.

CL-NET-04 · Belastbarkeit der Verwaltungsebene (DoS)

SOLL ☐

Anforderung: Die Verwaltungsebene drosselt übermäßige Verbindungsanfragen (Rate-Limiting, Kontingente) und hat ein dokumentiertes Verhalten für den eingeschränkten Betrieb unter Last.

Gründe: Die CRA fordert ausdrücklich Schutz gegen Überlastungsangriffe. Der praktische Grund: Wenn Ihre Fernwartung unter Angriff genau dann nicht mehr erreichbar ist, wenn Sie sie zur Abwehr dringend bräuchten, haben Sie im Ernstfall kein Werkzeug.

So wird geprüft: Belastungstest in der Teststellung: legitime Verbindungen müssen weiterhin möglich sein.

5.5 Protokollierung, Alarmierung, Nachvollziehbarkeit

Protokolle ohne Alarme sind wie Grabinschriften, die später erklären, was schiefging. Dieser Abschnitt gewährleistet, dass Sie im Falle eines Vorfalls eine angemessene Reaktion zeigen und im Nachhinein die erforderlichen Beweise sichern können.

CL-LOG-01 · Lückenlose Protokollierung sicherheitsrelevanter Ereignisse

MUSS · K.O. ☐

Anforderung: Alle Anmeldungen, erfolgreich und fehlgeschlagen, Sitzungen, Rechte- und Richtlinienänderungen werden zentral protokolliert, mit Personenidentität, Zeitstempel, Quell-Adresse und Ziel.

Gründe: Ohne Protokolle gibt es keine Aufklärung, keine Abgrenzung gegenüber Dienstleistern, keine Meldung an Behörden (NIS2/DSGVO) und keinen Versicherungsanspruch. Alle bisherigen Interviewpartner stuften die Protokollierung als unverzichtbar ein, zu Recht, denn sie ist das Rückgrat jeder anderen Kontrolle.

So wird geprüft: Führen Sie die Ereignisse einer Testsitzung durch und prüfen Sie den zugehörigen Protokolleintrag auf Vollständigkeit.

CL-LOG-02 · Manipulationssicher und ausreichend aufbewahrt

MUSS ☐

Anforderung: Protokolle sind manipulationssicher gespeichert. Die Aufbewahrungsdauer ist dokumentiert und aus dem Verwendungszweck, der Risikolage sowie rechtlichen und vertraglichen Pflichten abgeleitet, nach Ablauf erfolgt eine automatisierte Löschung oder Anonymisierung. Zugriffsrechte auf Protokolle sind geregelt, bestehende Aufbewahrungspflichten bleiben unberührt.

Gründe: Angreifer, die Spuren verwischen können, machen selbiges. Vorfälle werden oft erst Wochen oder Monate nach dem eigentlichen Angriff entdeckt: Zu kurze Aufbewahrung vernichtet Beweise, bevor der Vorfall überhaupt auffällt. Ungeprüft lange Aufbewahrung vergrößert umgekehrt das Datenvolumen, das bei einem Einbruch verloren geht. Entscheidend ist eine begründete, durchgesetzte Frist statt.

So wird geprüft: In einer vom Anbieter freigegebenen, isolierten Teststellung: Versuchen Sie als Administrator, einen Protokolleintrag zu löschen oder zu ändern. Dies muss scheitern oder versioniert und alarmiert werden. Prüfen Sie die dokumentierte Aufbewahrungs- und Löschkonfiguration gegen den Löschkalender.

CL-LOG-03 · Echtzeit-Alarme auf Hochrisiko-Ereignisse

MUSS (+ automatisierte Reaktion als SOLL) ☐

Anforderung: Die Lösung alarmiert nahezu echtzeitnah und ohne Sonderaufbau (z. B. an E-Mail/Teams/Slack) bei: neuer Geräte-Registrierung, gehäuften fehlgeschlagenen Anmeldungen, neu angelegten Administratorkonten, privilegierten Sitzungen auf Produktionssystemen, Sitzungen außerhalb der Geschäftszeiten, Deinstallationsversuchen und ungewöhnlichen Massenaktionen. *SOLL-Erweiterung:* automatische Gegenmaßnahmen (Konto sperren, Sitzung trennen) konfigurierbar.

Gründe: Fast alle schweren Vorfälle in Fernwartungssystemen waren im Protokoll sichtbar, nur hat sie niemand angesehen, weil niemand Protokolle live liest. Alarme bringen die entscheidenden Ereignisse präsent, statt dass man nach ihnen suchen muss.

So wird geprüft: Erzeugen Sie 5 fehlgeschlagene Anmeldungen in 10 Minuten; der Alarm muss in einem überwachten Kanal ankommen.

CL-LOG-04 · Exportierbare Protokolle

SOLL ☐

Anforderung: Protokolle lassen sich maschinenlesbar exportieren (syslog, API, Anbindung an Auswertungssysteme/SIEM); kein bloßer CSV-Klick-Download als einzige Möglichkeit.

Gründe: Für NIS2-Nachweise, DSGVO-Auskünfte, Versicherungen und die Zusammenarbeit mit Dienstleistern brauchen Sie Protokolldaten in auswertbarer Form. Nur-CSV-Export ist ein deutliches Reifegrad-Signal in die falsche Richtung.

So wird geprüft: Fordern Sie die Liste der Export-Schnittstellen an und testen Sie eine davon.

CL-LOG-05 · Synchronisierte Uhrzeiten

MUSS ☐

Anforderung: Alle Komponenten (Konsole, Vermittlungsdienst, Agenten) synchronisieren ihre Uhr mit einer gemeinsamen vertrauenswürdigen Zeitquelle (NTP). Zeitstempel sind über alle Protokolle konsistent.

Gründe: Ohne synchronisierte Uhren lässt sich die zeitliche Reihenfolge eines Vorfalles nicht rekonstruieren, vor allem dann nicht, wenn Ereignisse auf verschiedenen Systemen zusammengeführt werden sollen. Für forensische und behördliche Nachweise ist das unabdingbar.

So wird geprüft: Vergleichen Sie die Zeitstempel desselben Ereignisses (Sitzungsbeginn) in Agent-, Server- und Konsolen-Protokoll.

5.6 Notfallreaktion: Wenn es trotzdem passiert

Die folgenden Anforderungen behandeln den Tag, an dem Ihre Fernwartung selbst zum Angriffspfad wird. Dann zählt nur noch, wie schnell Sie sie abschalten und alle Schlüssel austauschen können, bevor Sie es brauchen.

CL-IR-01 · Dokumentierter Notfall-Abschalter (Kill-Switch)

MUSS ☐

Anforderung: Es existiert ein schriftlich dokumentiertes und regelmäßig geübtes Verfahren, das auch dann funktioniert, wenn die Fernwartungsebene selbst kompromittiert ist: Alle aktiven Sitzungen werden gekappt, Konten gesperrt und Agenten-Token widerrufen, unabhängig davon, ob die Verwaltungskonsole noch vertrauenswürdig ist. Netz- und EDR-Isolation der Agenten müssen separat von der RMM-Konsole durchführbar sein.

Gründe: Wenn ausgerechnet die Fernwartung der Angriffsweg ist, dürfen Sie die Abschaltung nicht allein über eben dieses Werkzeug fahren. Ein Verfahren, das nur auf Papier existiert, versagt im Ernstfall. Üben Sie es deshalb regelmäßig in einer vom Anbieter freigegebenen, isolierten Testumgebung.

So wird geprüft: Üben Sie das Verfahren in einer vom Anbieter freigegebenen, isolierten Testumgebung vollständig: Sitzungen enden, das Konto ist gesperrt, Token sind ungültig, und die Isolation greift auch ohne Konsole.

CL-IR-02 · Verfahren zum Austausch aller Zugangsdaten (Credential-Rotation)

MUSS ☐

Anforderung: Für den Ernstfall existieren dokumentierte und getestete Verfahren zum Austausch: der Server-Zertifikate/CA, der gerätespezifischen Agenten-Token, aller Administratoren-Zugänge und der Notfallkonten.

Gründe: Nach einem Anbieter-Einbruch wie bei AnyDesk oder TeamViewer ist der erste rationale Schritt, allen Komponenten das Vertrauen zu entziehen. Schritt zwei ist, alles Vertrauensmaterial auszutauschen. Fehlt das Verfahren, bleibt nach einem Vorfall nur ein manueller Neuaufbau.

So wird geprüft: Rotieren Sie in der Testumgebung Zertifikate und Token. Alte Zugangsdaten müssen danach abgewiesen werden.

CL-IR-03 · Forensischer Export je Sitzung

SOLL ☐

Anforderung: Zu einer konkreten Sitzung lassen sich Metadaten, Aufzeichnung und ausgeführte Befehle als zusammengehöriges Auswertungspaket exportieren.

Gründe: Für interne Untersuchungen, Versicherungen und behördliche Meldungen brauchen Sie die Geschichte einer spezifischen Sitzung als zusammenhängendes, überprüfbares Ganzes.

So wird geprüft: Exportieren Sie eine Testsitzung vollständig.

5.7 Datenschutz, Arbeitsrecht und Compliance

Fernwartung auf Geräten von Mitarbeitenden verarbeitet personenbezogene Daten und kann Verhalten überwachen, das berührt DSGVO und, wenn ein Betriebsrat existiert, dessen Mitbestimmung. Diese Anforderungen schützen Sie vor rechtlichen Fallstricken, über die Sie sonst erst im Streitfall erfahren.

CL-CMP-01 · Auftragsverarbeitungsvertrag und Prüfnachweise

MUSS ☐

Anforderung: Verarbeitet der Anbieter als SaaS-Lösung personenbezogene Daten in Ihrem Auftrag, existiert ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO. Der Anbieter weist ein unabhängig geprüftes Sicherheitsmanagement nach, als ISO-27001-Zertifizierung oder als SOC-2-Type-II-Bericht.

Gründe: Verarbeitet der Anbieter personenbezogene Daten in Ihrem Auftrag, ist diese Verarbeitung ohne AVV rechtlich nicht gedeckt. Unabhängig geprüfte Nachweise sind ein Anhaltspunkt dafür, dass der Anbieter Sicherheit organisiert betreibt.

So wird geprüft: Fordern Sie AVV-Muster und den aktuellen Prüfnachweis (Zertifikat bzw. Bericht) an.

CL-CMP-02 · Betriebsvereinbarung vor jeder Aufzeichnung/Überwachung

MUSS ☐

Anforderung: Bevor Sitzungsaufzeichnung oder Verhaltens-Protokollierung auf Geräten von Mitarbeitenden aktiviert wird, gilt: Besteht ein Betriebsrat und ist die Funktion geeignet, Verhalten oder Leistung zu überwachen, existiert eine Betriebsvereinbarung. In allen Fällen liegen ein dokumentierter Datenschutzhinweis (Zweck, Datenfelder, Zugriff, Aufbewahrung, Löschung) und eine dokumentierte Rechtsgrundlage vor. Tastaturaufzeichnung von Mitarbeitenden ist ohne besondere Rechtfertigung ausgeschlossen.

Gründe: Technische Einrichtungen, die geeignet sind, das Verhalten oder die Leistung von Mitarbeitenden zu überwachen, unterliegen nach § 87 Abs. 1 Nr. 6 BetrVG der Mitbestimmung. Nicht jede Fernwartung fällt automatisch darunter, die Einführung von Sitzungsaufzeichnung und Verhaltens-Protokollierung aber regelmäßig schon. Ohne Vereinbarung drohen Unterlassungsansprüche und ein Rechtsstreit, mit Vereinbarung gibt es Transparenz und Rechtssicherheit auf beiden Seiten.

So wird geprüft: Prüfen Sie vor Aktivierung jeder Aufzeichnungsfunktion den Zustand der Betriebsvereinbarung.

CL-CMP-03 · Aufbewahrung und automatische Löschung geregelt

MUSS ☐

Anforderung: Für Aufzeichnungen, Sitzungsprotokolle und personenbezogene Daten existiert ein dokumentierter Löschkalender mit aus Zweck, Risikolage und Vertragspflichten abgeleiteten Fristen, abgestimmt mit der Protokoll-Aufbewahrungsdauer, den die Lösung automatisch durchsetzt.

Gründe: Datenminimierung ist DSGVO-Grundsatz (Art. 5) und praktisch gesund: Je weniger alte Aufzeichnungen lagern, desto kleiner ist das Restrisiko bei einem Einbruch und desto einfacher jede Auskunft.

So wird geprüft: Konfigurieren Sie die Löschfrist und verifizieren Sie in der Teststellung das automatische Löschen.

CL-CMP-04 · Datenhaltung in der EU bzw. geprüfte Region

SOLL ☐

Anforderung: Sitzungsaufzeichnungen, Protokolle und personenbezogene Daten werden in der EU gespeichert, andernfalls liegt eine dokumentierte Bewertung der Datenübermittlung (Übertragungsinstrument wie Standardvertragsklauseln plus Einschätzung des Empfängerlands) vor.

Gründe: Datenabflüsse außerhalb der EU/EEA benötigen ein rechtliches Fundament (DSGVO Kapitel V). Seit "Schrems II" genügt eine Vertragsklausel allein nicht. Hinzu kommen eine Bewertung des Empfängerlands und gegebenenfalls ergänzende Maßnahmen. EU-Datenhaltung ist deshalb eine sinnvolle Bevorzugung und Risikominderung, aber nicht zwingendes Gebot: Auch Drittlandübermittlungen können rechtmäßig sein, wenn die Garantien des Kapitel V stimmen.

So wird geprüft: Frage: "In welcher Region werden unsere Daten (inkl. Backups, Protokolle, Aufzeichnungen) physisch gespeichert? Was bedeutet der Speicherort für die Sicherheit meiner Daten? Benennen Sie Subdienstleister."

CL-CMP-05 · Nachweistauglichkeit für Meldepflichten

SOLL ☐

Anforderung: Die Lösung unterstützt die Nachweis-Recherche für Meldungen: vollständige, schnell exportierbare Ereignisdaten zu einem Vorfall (wer, was, wann, betroffene Systeme), um NIS2-Fristen (24 h Frühwarnung / 72 h Meldung) und DSGVO (72 h an die Aufsichtsbehörde) einhalten zu können.

Gründe: Bei einem Vorfall gilt: Wenn Sie die Fakten nicht innerhalb von Stunden zusammenhaben, verpassen Sie Fristen, unabhängig davon, ob Sie selbst meldepflichtig sind oder es Ihre Kunden sind, die Auskunft von Ihnen verlangen.

So wird geprüft: Üben Sie den Export aller Ereignisse eines Testvorfalls mit Zeitstempel.

5.8 Anbieter, Updates und Lieferkette: Wem Sie vertrauen

Mit jeder Fernwartungslösung holen Sie sich einen Lieferanten tief in Ihr Vertrauensgefüge: Sein Server, seine Updates, sein Umgang mit Schwachstellen werden Teil Ihrer Sicherheit. Folgende Anforderungen machen das überprüfbar.

CL-GOV-01 · Nachprüfbare Sicherheitslage des Anbieters

SOLL ☐

Anforderung: Vor dem Kauf und danach jährlich prüfen Sie, wenn zutreffend: aktuelle ISO-27001-/SOC-2-Bescheinigung, eine öffentliche Meldestelle für Schwachstellen, vertragliche Benachrichtigungspflichten bei Sicherheitsvorfällen sowie, die einschlägige CVE-/Vorfallshistorie und wie der Anbieter damit umgegangen ist.

Gründe: Anbieter-Einbrüche schlagen auf Kunden durch. Sie können den Anbieter nicht sichern, aber Sie können wählen, mit wem Sie das Risiko teilen, und vertraglich sicherstellen, dass Sie es früh erfahren.

So wird geprüft: Fragen Sie nach Zertifikat, CVD-Kontakt und Meldeklausel, recherchieren Sie offenbare Sicherheitsvorfälle der letzten Jahre und deren Kommunikation.

CL-GOV-02 · Signierte Releases und Komponentenliste (SBOM)

SOLL ☐

Anforderung: Der Anbieter stellt Release-Prüfsummen/Signaturen bereit und liefert dem Käufer auf Anfrage eine aktuelle, maschinenlesbare SBOM (Software Bill of Materials, die Liste aller enthaltenen Bibliotheken/Komponenten), zu vereinbarten Vertraulichkeits- und Vertragsbedingungen.

Gründe: Wenn die nächste branchenweite Schwachstelle in einer verbreiteten Bibliothek auftaucht, beantwortet die SBOM die Existenzfrage in kürzester Zeit. Die CRA verpflichtet **Hersteller**, eine SBOM zu erstellen und Marktüberwachungsbehörden auf begründeten Antrag Informationen bereitzustellen. Eine allgemeine Veröffentlichungspflicht gegenüber Kunden ergibt sich daraus nicht, fordern Sie die SBOM deshalb vertraglich an.

So wird geprüft: Fordern Sie SBOM und Signaturinformationen für die aktuelle Release an.

CL-GOV-03 · Sicherheitsupdates zugesagt und getrennt von Funktionen

SOLL ☐

Anforderung: Der Anbieter stellt Sicherheitsupdates unverzüglich, getrennt von Funktions-Updates und normalerweise kostenfrei bereit und benennt verbindliche Reaktionszeiten auf bekannt werdende Schwachstellen.

Gründe: Ausgenutzte, aber längst gepatchte Schwachstellen sind ein wiederkehrendes Muster: Nach Bekanntwerden der ScreenConnect-Schwachstelle und Verfügbarkeit des Fixes wurden verwundbare, internetseitig erreichbare Installationen rasch angegriffen; zügiges Patchen zählt. Ihre Sicherheit steht und fällt damit, ob Ihr Anbieter Sicherheitsprobleme schnell und sauber behebt und ob Sie die Updates einspielen.

So wird geprüft: Vertragliche Formulierung einfordern. Historie prüfen ("Wie schnell erschienen die letzten drei Sicherheits-Updates?").

CL-GOV-04 · Supportzeitraum vertraglich benannt

MUSS ☐

Anforderung: Vertraglich ist festgehalten, bis wann Sicherheitsupdates und Schwachstellenbehebungen für die gekaufte Version gewährleistet sind, und was danach gilt.

Gründe: Eine Lösung ohne laufenden Sicherheits-Support ist ein immer weiter wachsendes Risiko. Die CRA verpflichtet Hersteller, den Supportzeitraum offenzulegen.

So wird geprüft: Supportende für Ihre Version schriftlich bestätigen lassen.

CL-GOV-05 · Sichere Standardkonfiguration mit Zurücksetzbarkeit

MUSS ☐

Anforderung: Die Lösung ist ab Werk sicher vorkonfiguriert (Verschlüsselung an, Aufzeichnungsfunktion und Übertragungsfunktionen geregelt, keine Standard-Kennwörter) und kann auf diese sichere Grundeinstellung zurückgesetzt werden.

Gründe: Die sicherste Funktion nützt nichts, wenn sie nach der Installation erst gefunden und aktiviert werden muss, erst recht ohne IT-Sicherheitsabteilung. Fehlkonfiguration ist die typischste KMU-Schwachstelle, sichere Defaults beseitigen sie an der Wurzel. Zugleich ist dies eine CRA-Anforderung an Produkte.

So wird geprüft: Installieren Sie in einer frischen Teststellung und prüfen Sie, welche der MUSS-Anforderungen ohne Zutun erfüllt sind. Frage nach dem Zurücksetzen auf Werks-Sicherheitsstand.

5.9 Speziell: Fernwartung durch externe Dienstleister auf Ihren Systemen (Fall B)

Wenn ein Maschinenhersteller oder Dienstleister per Fernwartung auf Ihre Anlagen, Steuerungen oder Rechner zugreift, sind Sie Betreiber und tragen die Verantwortung, auch wenn die Software beim Dienstleister läuft. Genau dieses Szenario stand im Zentrum der bisherigen Interviews mit Unternehmen aus dem Maschinen- und Anlagenbau. Der BSI-Baustein OPS.1.2.5 "Fernwartung" liefert die Grundlage für diesen Abschnitt, insbesondere seine Anforderung A19 "Fernwartung durch Dritte".

CL-EXT-01 · Aktive Freigabe jeder Sitzung durch Ihre Seite

MUSS · K.O. ☐

Anforderung: Jede Dienstleister-Sitzung auf Ihren Systemen benötigt die aktive Freigabe durch Ihre Seite (Ihr Personal bestätigt den Zugriff, bevor die Verbindung steht). Eine unverzügliche, deutlich sichtbare Benachrichtigung mit der Möglichkeit, sofort zu beenden, ersetzt die aktive Freigabe nie. Unbegleitete Zugriffe (etwa auf Server ohne anwesende Personen) sind nur als gesondert konfigurierte, besonders gesicherte Ausnahme zulässig.

Gründe: Die Angreifer-Szenarien "gestohlener Dienstleister-Zugang" und "unbemerkte Sitzung nachts" funktionieren nur, wenn niemand auf Ihrer Seite zustimmen und stoppen muss. Aktive Freigabe gehörte in den Interviews zu den am häufigsten geforderten Funktionen, als ER.5 ist sie auch in der BSI-TR-01393 gefordert.

So wird geprüft: Lassen Sie den Dienstleister eine Testsitzung öffnen: ohne Ihre Freigabe darf keine Verbindung entstehen.

CL-EXT-02 · Verbindung wird von Ihrer Seite initiiert

MUSS ☐

Anforderung: Der Verbindungsaufbau geht von Ihrem Netz aus (das System meldet sich nach außen, Rendezvous-Prinzip) oder über einen beidseitig angesprochenen Vermittlungsdienst. Auf Ihrer Seite sind keine eingehenden Firewall-Freigaben für den Dienstleister nötig.

Gründe: Jede eingehende Freigabe zu Ihren Maschinen ist eine dauerhafte, von außen testbare Tür. Das Rendezvous-Modell macht Ihre Systeme von außen unsichtbar.

So wird geprüft: Prüfen Sie Ihre Firewall-Regeln an der Maschine: keine eingehenden Regeln; die Fernwartung funktioniert dennoch.

CL-EXT-03 · Befristete Zugänge statt Dauerberechtigung

MUSS ☐

Anforderung: Dienstleister-Zugänge sind zeitlich befristet (auf die Wartungssitzung oder den Wartungstag) und werden danach automatisch ungültig. Dauerhafte Zugänge existieren nur als dokumentierte, besonders überwachte Ausnahme.

Gründe: Ein Dauertunnel zu einem externen Dienstleister ist eine stehende Einbruchsstelle, an der Sie keine Kontrolle haben, und ein beliebtes Ziel, weil dort oft schwächere Konten liegen. Befristung räumt die Tür nach dem Besuch wieder ab.

So wird geprüft: Prüfen Sie, dass der Zugang nach Ablauf einer Testsitzung bzw. des Zeitfensters automatisch ungültig wird.

CL-EXT-04 · Vertragliche Sicherheitsregeln mit dem Dienstleister

MUSS ☐

Anforderung: Mit jedem fernwartenden Dienstleister bestehen schriftliche Vereinbarungen, die mindestens regeln: Zugriff nur auf die vereinbarten Systeme; Protokollierung der Zugriffe und Ihre Einsichtsrechte; unverzügliche Meldung von Sicherheitsvorfällen und Schwachstellen, die den Fernwartungsweg betreffen; keine Weitergabe des Zugangs an Dritte.

Gründe: Technische Kontrollen haben nur eine begrenzte Wirksamkeit, wenn das Ziel effektive Arbeit ist. NIS2 macht die Lieferkette ausdrücklich zum Prüfpunkt, und im Vorfall brauchen Sie Melde- und Auskunftsansprüche, die Sie jetzt, in Ruhe, vereinbaren.

So wird geprüft: Prüfen Sie die Verträge Ihrer Partner gegen diese vier Mindestpunkte.

CL-EXT-05 · Eigene Protokollierung und Kontrolle der Zugriffe

MUSS ☐

Anforderung: Sie führen selbst (oder über die gemeinsam genutzte Lösung) ein Verzeichnis aller Fernwartungszugriffe auf Ihre Systeme (welcher Dienstleister, wann, auf welche Anlage, wie lange, mit welchem Anlass) und können Sitzungen bei Bedarf selbst beobachten oder beenden.

Gründe: Vertrauen ist gut, Kontrolle ist besser. Der BSI-Baustein verlangt, dass externe Fernwartung durch eigenes Personal beobachtet und protokolliert wird. Nur so können Sie im Streit- oder Schadensfall differenzieren, was über den Dienstleister-Weg geschah und im Notfall selbst handeln, wenn der Dienstleister gerade nicht erreichbar ist.

So wird geprüft: Prüfen Sie, wo das Zugriffsverzeichnis Ihrer Anlagen liegt und wer es einsehen kann; üben Sie die Beendigung einer laufenden Dienstleister-Sitzung.

CL-EXT-06 · Getrennter Zugangsweg und Vier-Augen-Prinzip bei OT

SOLL ☐

Anforderung: Bei industriellen Anlagen/Steuerungen (OT) läuft die Fernwartung über einen abgetrennten Übergang (eigener Verwaltungsnetz-Bereich, Sprungserver in einer DMZ an der IT/OT-Grenze), nicht direkt aus dem Büro-Netz. Für sicherheitsrelevante Maschinen gilt ein Vier-Augen-Prinzip: Ihre Fachkraft kann die Sitzung live mitverfolgen und unterbrechen.

Gründe: Eine Fehlbedienung oder Kompromittierung an einer Produktionsanlage kostet nicht nur Daten, sondern Stillstand, Material und Sicherheit der Menschen. Der getrennte Weg begrenzt, was von der IT-Seite in die Fertigung reicht; das Vier-Augen-Prinzip stellt sicher, dass immer jemand Ihrerseits zusieht, der die Anlage kennt.

So wird geprüft: Architektur-Skizze des Fernwartungswegs bis zur Anlage anfordern; Rollen für "mitsehende Fachkraft" konfigurieren und testen.

5.10 Speziell: Betrieb für mehrere Kunden (Dienstleister/MSP, Fall C)

Nur relevant, wenn Sie als Dienstleister die Fernwartung mehrerer Kunden auf einer gemeinsamen Plattform betreiben.

CL-TEN-01 · Strikte Mandantentrennung

MUSS, falls zutreffend ☐

Anforderung: Daten und Geräte jedes Kunden (Gerätelisten, Skripte, Aufzeichnungen, Protokolle) sind logisch oder physisch voneinander getrennt; ein Zugriff über Mandantengrenzen hinweg ist ohne ausdrückliche, dokumentierte Delegation technisch unmöglich.

Gründe: Ein Dienstleister, bei dem alle Kunden in einem Topf liegen, macht einen einzigen Fehler für alle zum Vorfall. Der Kaseya-Vorfall war genau das: rund 60 direkt betroffene Dienstleister, rund 1.500 betroffene Endkunden. Eine Trennung begrenzt den Schaden auf den betroffenen Mandanten.

So wird geprüft: Versuchen Sie als Administrator eines Test-Mandanten, Geräte eines anderen Mandanten aufzulisten oder per ID-Raten zu erreichen: beides muss abgewiesen und protokolliert werden.

CL-TEN-02 · Mandantenbezogene Rollen

SOLL ☐

Anforderung: Administratoren Ihrer Kunden sehen und verwalten ausschließlich ihre eigenen Geräte und Benutzer, mit eigenen Rollen.

So wird geprüft: Anmeldungen mit zwei Test-Mandanten-Administratoren vergleichen.

5.11 Organisatorische Grundlagen in Ihrem Unternehmen: Auch die beste Lösung reicht nicht allein

Die folgenden Punkte lassen sich in der Regel nicht einkaufen: Sie beschreiben, was Sie selbst regeln müssen. Sie sind bewusst knapp gehalten, jede Lösung erfordert nur Entscheidungen und ein paar Stunden Arbeit, aber ohne sie bleiben selbst abgehackte technische Anforderungen wirkungslos.

CL-ORG-01 · Schriftliche Fernwartungsrichtlinie

MUSS ☐

Anforderung: Eine kurze, unterschriebene Richtlinie regelt: Wer darf Fernwartungssitzungen starten (Rollen), auf welche Systemklassen, mit welcher Freigabe, zu welchen Zeiten, wie Sitzungen aufgezeichnet und geprüft werden und dass jede Sitzung einem Anlass/Ticket zugeordnet wird.

Gründe: Ohne schriftliche Regel ist jede technische Kontrolle isoliert und im Streitfall nicht nachvollziehbar. Die NIS2 fordert eine Richtlinie, und der Ticket-Bezug ist Ihr Hebel, um geplante von ungeplanten Sitzungen zu unterscheiden.

CL-ORG-02 · Nur freigegebene Fernwartungs-Tools, alles Übrige blockiert

MUSS ☐

Anforderung: Auf Ihren verwalteten Geräten ist ausschließlich die freigegebene Fernwartungslösung erlaubt; alle anderen Fernzugriffs-Programme werden per Anwendungs-Kontrolle blockiert und bei Auftreten alarmiert. Die Sperrung muss auch portable, nicht installierte Programme aus benutzerbeschreibbaren Verzeichnissen umfassen.

Gründe: Betrüger überreden Mitarbeitende per Anruf, ein völlig legales Fernwartungsprogramm zu starten, das Programm braucht keine Installation und löst keine Virenschutz-Warnung aus. Technische Blockierung plus geschulte Mitarbeitende schließen genau diese Lücke.

So wird geprüft: Versuchen Sie auf einem Testgerät, ein fremdes Fernwartungsprogramm (installiert und als portable Kopie) zu starten. Beides muss blockiert und gemeldet werden.

CL-ORG-03 · Eigener Patch-Prozess mit festen Fristen

MUSS ☐

Anforderung: Sie pflegen die Fernwartungs-Infrastruktur selbst nach festen Fristen: Notfall-/überall ausgenutzte Schwachstellen (Orientierung: CISA KEV) innerhalb von 72 Stunden, hohe Schweregrade innerhalb von 14 Tagen, übrige innerhalb von 30 Tagen. Der Patch-Stand wird monatlich geprüft. Bei SaaS prüfen Sie, dass der Anbieter liefert, und ziehen Updates zeitnah auf die Geräte.

Gründe: Der häufigste Grund, warum gepatchte Schwachstellen trotzdem Schaden anrichten: niemand spielte den Patch ein. Die Angriffswellen auf ScreenConnect und ManageEngine trafen überwiegend Systeme, für die längst ein Update verfügbar war.

So wird geprüft: Legen Sie die Fristen schriftlich fest, prüfen Sie monatlich den Versionsstand gegen die Herstellerhinweise, abonnieren Sie Sicherheits-Advisories der Hersteller.

CL-ORG-04 · Benannte Verantwortliche und geübte Abläufe

MUSS ☐

Anforderung: Eine namentlich benannte Person ist für den Ernstfall der Fernwartung zuständig (Ansprechpartner, Entscheidungsbefugnis); die Notfall- und Rotations-Verfahren werden mindestens jährlich geübt, inklusive eines Szenarios "Anbieter kompromittiert".

Gründe: Im Vorfall entscheidet nicht das Dokument, sondern der geübte Ablauf. NIS2 macht die Vorsorge und Übung zur Führungsaufgabe. Eine Übung ist der einzige Moment, in dem Sie die Lücken im Verfahren gefahrlos finden.

CL-ORG-05 · Betriebsrat und Datenschutzbeauftragte vorab einbinden

MUSS ☐

Anforderung: Vor der Einführung werden Betriebsrat (falls vorhanden) und Datenschutzbeauftragte einbezogen: Betriebsvereinbarung für Aufzeichnung/Überwachung, Datenschutz-Dokumentation. Bei Funktionen mit KI-Elementen (z. B. automatische Chat-

Übersetzung in der Sitzung) zusätzlich eine dokumentierte Schwellenwertprüfung: Ergibt sie ein voraussichtlich hohes Risiko, folgt eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO).

Gründe: Die Anforderungen aus Interviews enthalten Funktionen, die datenschutz- und arbeitsrechtlich anspruchsvoll sind. Wartungsschat-Inhalte an einen KI-Dienstleister zu leiten, ist ein Verarbeitungsschritt, der bewertet werden will.

CL-ORG-06 · Gestufter Rollout und Test vor dem Produktivbetrieb

SOLL ☐

Anforderung: Die Einführung erfolgt gestuft: kurze Pilotphase auf wenigen Geräten, Prüfung der kritischen Einstellungen anhand der Abnahmetests, Test des Notfall-Abschalters, dann erst Ausrollung auf die Flotte.

Gründe: Ein Konfigurationsfehler auf einem Gerät ist korrigierbar, derselbe Fehler auf 200 Geräten ist kritisch. Der Test des Kill-Switch vor Produktivstart wäre ein günstigste Moment, um festzustellen, dass er nicht funktioniert.

CL-ORG-07 · Mitarbeitende sensibilisieren

SOLL ☐

Anforderung: Ihre Mitarbeitenden kennen die Grundregel: Aufforderungen am Telefon (Installation eines Fernzugriffs-Programms, Vorlesen von Codes) werden nicht direkt ausgeführt, sondern über einen bekannten, verifizierten Kanal bestätigt (z. B. internes Ticket oder Rückruf über eine bekannte Nummer). Sensibilisierung hilft, solche Anrufe zu erkennen und abzuweisen, sie ersetzt keine technische Sperrung. Ihre Mitarbeitenden wissen, wie eine legitime Fernwartungssitzung aussieht (Banner, Name, Beenden-Möglichkeit) und an wen sie Verdachtsfälle melden.

Gründe: Der technische Schutz greift nur, wenn er aktiv ist, der Betrugsanruf zielt auf den Moment, in dem eine Person "hilft". Sensibilisierung hilft und ist eine kostengünstige Maßnahme.

6. Quellen und Herleitung

Jede Anforderung dieser Anforderungsscheckliste stammt aus einer von drei Quellgruppen:

- 1. **Fern-Compass-Framework:** Eingehende Expertentips als technische Detailbegründung nebst Prüfanleitungen.
- 2. **Interview-Spezifikation:** Interviews mit Unternehmen des technischen Service.
- 3. **Normen und Regulierung:** BSI IT-Grundschutz (OPS.1.2.5 "Fernwartung", IND.3.2, ORP.4), 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 der zugehörigen BSI-TR-01383.

7. Glossar

Begriff	Bedeutung
Agent	Kleines Programm auf jedem gewarteten Gerät; hält die Verbindung zur Verwaltungskonsole und führt Aktionen aus.

Begriff	Bedeutung
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.

8. 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.