AEB SE

Servicebeschreibung Fernwartung

Version 1.1

1.1.2021

www.aeb.com

AEB

Inhalt

Präambel

Sowohl für die Implementierungsphase unserer Lösung bei Ihnen als auch für den anschließenden reibungslosen Betrieb ist eine funktionierende Fernwartungsanbindung ein wichtiger Baustein für kurze Projektlaufzeiten und schnelle Lösungsfindung im Problemfall sowie für die Einhaltung von abgeschlossenen SLAs notwendig.

1 Sicherheit und berechtigte Personen bei AEB

Generell gilt, dass sich alle Mitarbeitenden der AEB persönlich zur Geheimhaltung verpflichtet haben. Diese Verpflichtung gilt sowohl für die AEB sowie gegenüber all unseren Kunden.

Die eingegangene Verpflichtung kann vom AEB-Mitarbeitenden nur dem Arbeitgeber gegenüber erbracht werden, nicht gegenüber Dritten (Dienstherrenprinzip). Zudem hat AEB auch ihren Mitarbeitenden gegenüber den Datenschutz zu wahren.

Aus diesem Grunde sichert AEB folgende Verfahrensweise und -sicherheit für Kunden-Fernwartungen zu:

1. Für den Zugriff auf ein Kundensystem muss immer ein Grund vorliegen. Diese Notwendigkeit im Regelbetrieb wird in einem Ticket innerhalb eines AEBTicketsystems dokumentiert. Projektbezogene Fernwartungszugriffe erfolgen in Absprache mit dem Projektleiter oder dem Projekt-Team.
2. AEB verwaltet Passwörter oder andere, sicherheitskritische Fernwartungsdaten mit Hilfe eines Passwort-Tools, das Zugriffe für AEB-Mitarbeitende reglementiert und nur berechtigten Personen protokolliert Zugriff darauf erteilt.
3. Passwortdaten und andere, sicherheitskritische Fernwartungsdaten werden nicht im Klartext gespeichert.
4. Zugriffe auf Kundensysteme erfolgen ausschließlich aus gesicherten Netzwerken der AEB. Im Einsatz befindliche Next-Generation-Firewalls und -Virenscanner werden ständig durch AEB überprüft und auf Basis aktueller Bedrohungsszenarien permanent optimiert und gewartet.

Im Bedarfsfall kann AEB die durchgeführten Zugriffe inklusive beteiligte AEB-Mitarbeitende, Tickets und Dauer auflisten und auf Nachfrage zur Verfügung stellen.

Im Regelbetrieb erbringen eine Vielzahl von Mitarbeitenden Service und Support, teilweise auch im Mehrschichtbetrieb und von unterschiedlichen Standorten aus. Alle diese Mitarbeitenden unterstehen ausnahmslos den oben genannten Verschwiegenheits- und Datenschutzerklärungen.

2 Technische Verbindung

AEB bietet folgende Varianten für die Fernwartungsverbindung zu Kunden an. Die zuerst genannten Varianten passen aus AEB-Sicht insgesamt erfahrungsgemäß am besten bzgl. initialem und laufendem Aufwand, um so möglichst wenig Verzögerung im Projekt und bei Support-Fällen zu verursachen.

2.a TeamViewer

Webbasierte Standard-Anwendung für Fernwartungen über das Internet. Für die Ad-Hoc-Variante ist keine Installation notwendig, der Client wird im Bedarfsfall im Browser von einem Mitarbeitenden des Kunden aufgerufen. Für die „TeamViewer-Host"-Variante ist die Installation eines Dienstes auf (mindestens) einem der fernzuwartenden Kundenserver notwendig.

Vorteile:

- Keine Einrichtung notwendig (außer bei der Variante „TeamViewer Host")
- Schnelle Verbindung über das Internet nach Freigabe durch den Benutzer

Nachteile (außer bei der Variante „TeamViewer-Host"):

- Der Anwender muss die Fernwartung aktiv öffnen und den Prozess der Analyse und Fehlerbehebung begleiten. Arbeiten an diesem Fernwartungsrechner ist während dieser Zeit nicht möglich.
- Längere Analysen können unter Umständen auch mehrere Zugriffe benötigen, die dann gemeinsam geplant werden müssen.
- Servicefallbearbeitung zu Randzeiten oder mit Analyse-Unterbrechungen (z. B. durch interne Rückfragen) werden erschwert bzw. sind nicht möglich.
- Übergabe der Fernwartung an einen Entwickler oder ein Produkt-Team zur weiteren Analyse ist nicht oder nur sehr schwer möglich.

2.b Site-2-Site VPN (LAN-LAN-Kopplung)

Netzwerkkopplung über eine abgesicherte VPN-Anbindung auf Router-Ebene, die einen

Zugriff per RDP, SAP®-GUI o. ä. (je nach Bedarf) aus dem AEB-Netz auf die fernzuwartenden

Kundenserver ermöglicht.

Vorteile:

- Schneller Zugriff auf die installierten AEB-Systeme beim Kunden
- Bessere Lösungs- und Supportzeiten bei komplexen Problemen, ggf. auch in Rand- und Sonderzeiten hinein
- Kein aktives Eingreifen auf Kundenseite zur Öffnung der Fernwartung nötig
- Sichere, getunnelte Lösung ohne Einsatz von Fremdsoftware
- Schnelles Teamworking mit Produkt- und Entwicklungskollegen bei komplexen Fehlersituationen

Nachteile:

- Initial geringfügig höherer Aufwand bei der Einrichtung

2.c Terminal Server basierter Zugang

Z. B. per Citrix oder RDP zu gepublishten Anwendungen oder Desktops, die eine Fernwartung (Web-Browser, SAP®-GUI, RDP-Verbindungen etc.) ermöglichen.

Vorteile:

- Ggf. kein aktives Eingreifen auf Kundenseite zur Öffnung der Fernwartung nötig
- Zwei-Faktor-Authentifizierung möglich, wenn gewünscht

Nachteile:

- Initialer Einrichtungsaufwand
- Laufender Pflegeaufwand auf Kundenseite
- Ggf. initiale und/oder laufende Kosten für Lizenzen und/oder Tokens
- Ggf. keine Datenübertragung möglich, dadurch erschwerte Analyse von Logs durch Produkt- oder Entwicklungsteams

2.d VPN-Client in einer Fernwartungs-DMZ bei AEB

Einsatz eines VPN-Clients, der eine verschlüsselte VPN-Verbindung zum Kundennetz

aufbaut.

Voraussetzungen:

- Split-Tunneling muss dafür auf Kundenseite zwingend erlaubt sein
- Der vom Kunden bereitgestellte VPN-Client muss vorab von AEB bzgl. Kompatibilität und Verwendbarkeit in der Fernwartungs-DMZ geprüft werden

Vorteile:

- Ggf. kein aktives Eingreifen auf Kundenseite zur Öffnung der Fernwartung nötig
- Zwei-Faktor-Authentifizierung möglich, wenn gewünscht

Nachteile:

- Nutzung einer speziellen Fernwartungs-DMZ auf AEB-Seite aus Kompatibilitäts- und Sicherheitsgründen
- Deutlich erhöhter initialer Einrichtungsaufwand
- Erhöhter laufender Pflegeaufwand auf Kunden- und AEB-Seite
- Erhöhte Reaktionszeit im Projekt und bei Support-Fällen durch aufwändigeren und fehleranfälligeren Verbindungsaufbau

- Ggf. initiale und/oder laufende Kosten für Lizenzen und/oder Tokens
- Ggf. keine Datenübertragung möglich, dadurch erschwerte Analyse von Logs durch Produkt- oder Entwicklungsteams

3 Authentifizierung

Für die Verbindungs-Authentifizierung bei den Fernwartungsvariante 2.c und 2.d gibt es drei gängige Varianten:

3.a Authentifizierung über Benutzername/Passwort

Zugangsdaten werden in einem Passwort-Tool bei AEB hinterlegt (siehe Kapitel 1) und im Bedarfsfall verwendet. Der Zugriff auf die Zugangsdaten in diesem Passwort-Tool ist dabei auf berechtigte Personen eingeschränkt.

3.b Zwei-Faktor-Authentifizierung über Hardware-Token

Der Kunde überlässt AEB einen Hardware-Token, der von AEB zur Authentifizierung verwendet wird.

3.c Zwei-Faktor-Authentifizierung über Soft-Token oder Spezial-App

Auf Kundenwunsch kann ergänzend zu Benutzerdaten und Passwörtern ein zweiter Faktor über einen Soft-Token oder eine Spezial-App generiert werden. Entsprechende Token-Generatoren und Spezial-Apps müssen von der AEB vorab auf Kompatibilität überprüft werden.

Eine Zwei-Faktor-Authentifizierung über einen Telefonanruf oder eine SMS ist nicht möglich und wird von AEB daher nicht unterstützt. FIDO2 (z. B. Yubi-Key) Varianten müssen vorab von AEB geprüft werden.

AEB empfiehlt aus jahrelanger Erfahrung im Betrieb und bei Kundenprojekten die Fernwartungsvariante 2.b, also die Einrichtung einer Site-2-Site-VPN-Verbindung zum Zugriff per RDP oder SAP®-GUI auf Kundenserver mit AEB-Komponenten. Um auch bei Supportfällen in Randzeiten die Reaktionszeit möglichst gering zu halten, wird zur Authentifizierung ein nicht personalisierter Zugangsuser bevorzugt, der im AEB-Passwort-Tool hinterlegt werden kann.

AEB SE

Hauptsitz . Sigmaringer Straße 109 . 70567 Stuttgart . Deutschland . +49 711 72842 0 . www.aeb.com . info.de@aeb.com . Registergericht: Amtsgericht Stuttgart . HRB 767 414 . Geschäftsführende Direktoren: Matthias Kieß, Markus Meißner . Vorsitzende des Verwaltungsrats: Maria Meißner

Standorte

Düsseldorf . Hamburg . Lübeck . Mainz . Malmö . München . New York . Prag . Rotterdam . Salzburg . Singapur . Soest . Stuttgart . Warwick . Zürich