ISONA Fernwartungssystem

Erhöhte Anforderungen bezüglich IT-Security (z.B. NIS-2) erfüllen

Das **ISONA Fernwartungssystem** ist eine innovative Lösung, die mit einem hohen Sicherheitsstandard alle erdenklichen Anforderungen in unterschiedlichsten Einsatzszenarien abdeckt. Durch das flexible Konzept des Systems lassen sich auch komplexe, kundenspezifische Prozesse abbilden.
Speziell für KRITIS-Unternehmen, Firmen mit Maschinenparks/Geräten unterschiedlicher Hersteller aber auch für Firmen mit heterogenen Serverumgebungen, die externe Dienstleister zu Wartungszwecken sicher auf ihre Maschinen / Server zugreifen lassen möchten, ist das **ISONA Fernwartungssystem** optimal geeignet.

Die folgende Grafik erläutert den Aufbau des ISONA Fernwartungssystems:

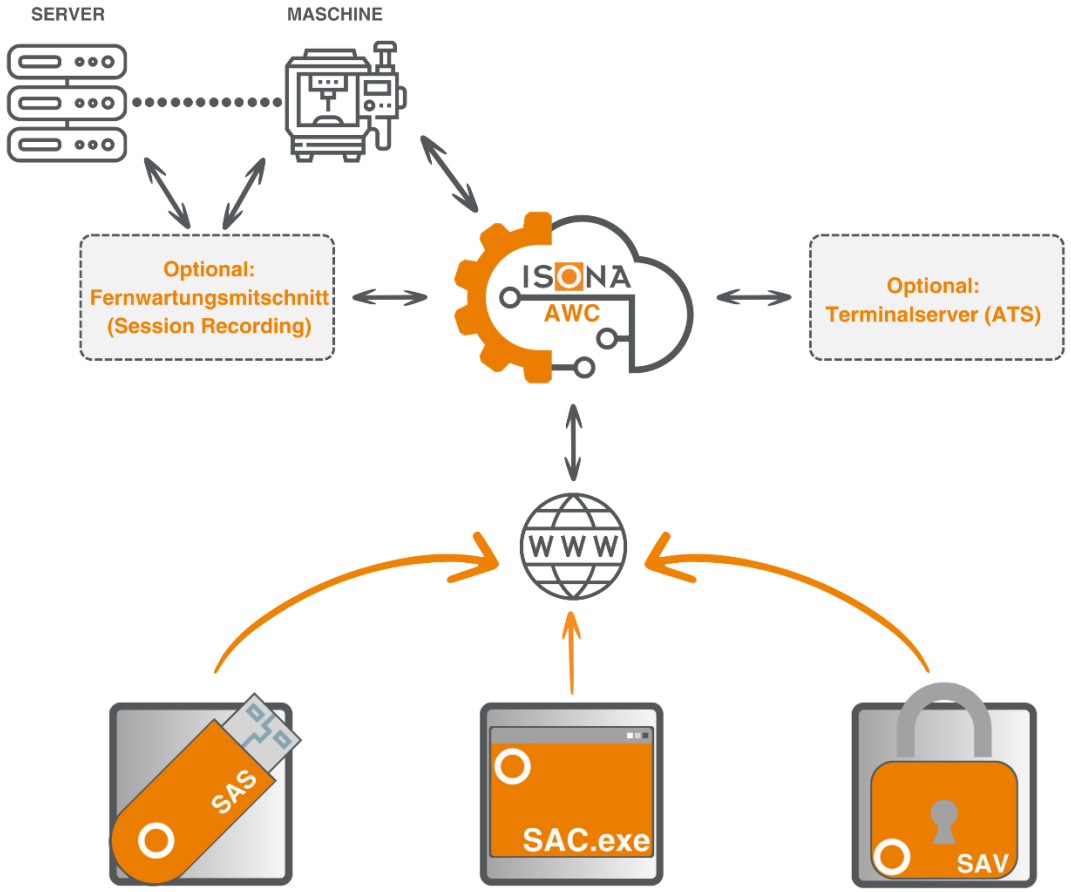

Abb. 1: Komponenten des ISONA Fernwartungssystems

Das ISONA Fernwartungssystem umfasst folgende Funktionen:

- ⇨ Login von externen Servicetechnikern im Fernwirkportal, um Fernwartungsanfrage zu stellen
- ⇨ Freigabe einer Fernwartungsanfrage durch einen Mitarbeiter in der Firma (auch via Smartphone)
- ⇨ Zeitliche Limitierung der Fernwartungssitzung durch automatische Beendigung des VPN-Tunnels
- ⇨ Revisionssicherer Mitschnitt der Fernwartungssitzung mit dem optionalen Session Recording System
- ⇨ Inventarsystem, in dem alle Informationen über Server und Maschinen erfasst sind
- ⇨ Adressverwaltung mit den Kontaktdaten von Herstellern, Servicepartnern usw.
- ⇨ Automation WebCenter (AWC) basierend auf SQL-Datenbank mit Schnittstellen zu übergeordneten Applikationen
- ⇨ Einfache VPN-Konfiguration der Endgeräte über das Automation WebCenter (AWC) durch den Endbenutzer

Gesamtübersicht

Version 1.6

Nachfolgend werden die einzelnen Komponenten des ISONA Fernwartungssystems beschrieben:

Komponente 1: Automation WebCenter (AWC) mit integriertem Secure Access Gateway (SAG)

Das Secure Access Gateway (SAG) stellt die zentrale IT-Security-Komponente des ISONA Fernwartungssystems dar. Es dient als VPN-Gateway, Fernwartungsserver, Authentisierungsserver, Berechtigungssystem, Routingserver sowie als zentraler Managementserver für alle Komponenten des ISONA Fernwartungssystems. Das Secure Access Gateway wird als virtuelle Appliance (lauffähig auf VMware®, Hyper-V®, XenServer®, Oracle VirtualBox®) beim Kunden hinter der Firewall oder in der DMZ installiert (2-stufiges Sicherheitskonzept).

Komponente 2: Secure Access Stick (SAS)

Der Secure Access Stick (SAS) erlaubt es, von extern sicher auf beliebige Server, Maschinensteuerungen usw. per RDP, VNC o.ä. zuzugreifen. Dieser spezielle USB-Stick benötigt keinerlei Installation oder Adminrechte und hinterlässt auf dem Windows®-Gastsystem keine Spuren, da er in einer abgeschirmten Umgebung (Sandbox) läuft. Sämtliche Software, die der Anwender benötigt um eine sichere VPN-Verbindung aufzubauen und auf die vorhandene Infrastruktur zuzugreifen, ist bereits auf dem Stick integriert. Dieser ermöglicht zusammen mit dem Kennwort eine hochsichere 2-Faktor-Authentifizierung (2FA) des Benutzers.

Komponente 3: Secure Access Client (SAC)

Der Secure Access Client (SAC) ist die USB-sticklose Variante des Secure Access Stick (SAS) mit identischen Features. Dadurch wird auch ein Zugang von Windows®-PCs aus ermöglicht, bei denen eine Nutzung von USB-Sticks nicht erlaubt ist oder wenn explizit ein alternativer Zugang gewünscht ist.
Sämtliche Software, die der Anwender benötigt um eine sichere VPN-Verbindung aufzubauen und auf die Server/Maschinen zuzugreifen, wird nach der Authentisierung von dem Secure Access Gateway (SAG) auf den Gast-PC geladen und in einer abgeschotteten Sandbox ausgeführt.
Für die sichere 2-Faktor-Authentifizierung (2FA) des Benutzers kann je nach Anforderung entweder ein OTP-Token (**O**ne**T**ime**P**assword = Einmalkennwort), ein Soft-Token (Kennwort-App auf einem Smartphone wie z.B. Google Authenticator), eine OTP-SMS (Einmalkennwort via SMS) oder OTP-Mail (Einmalkennwort via E-Mail) verwendet werden. Die Verwaltung der unterschiedlichen OTP-Varianten erfolgt zentral im Secure Access Gateway (SAG).

Komponente 4: Secure Access VPN (SAV)

Mit dem Secure Access VPN (SAV) ist ein sicherer Fernwartungszugriff auf Server/Maschinen von Tablets oder Smartphones aus möglich. Der Secure Access VPN basiert auf dem OpenVPN Client und ist damit auf allen Endgeräten lauffähig mit den Betriebssysteme Windows, MAC, IOS, Android und Linux.
Für eine sichere Authentisierung des Benutzers wird der Secure Access VPN ergänzt um eine 2-Faktor-Authentifizierung (2FA) mit einem Einmalkennwort. Für das Einmalkennwort stehen die gleichen Varianten wie beim Secure Access Client (siehe oben) zur Verfügung.

Komponente 5: Fernwartungsmitschnitt

Um z.B. NIS-2 Anforderungen zu erfüllen, wird eine virtuelle Appliance für den Fernwartungsmitschnitt (Session Recording) in den Datenstrom zu den Servern/Maschinen eingebunden. Diese zeichnet die Protokolle HTTP(S), RDP, VNC, ICA, SSH und Telnet auf. Damit lässt sich später genau nachweisen, was der externe Benutzer auf dem Server/der Maschine konfiguriert und installiert hat. Das System unterstützt auch das Vier-Augen-Prinzip, bei dem man zeitgleich mitverfolgen kann, was der externe Benutzer auf dem Zielsystem gerade arbeitet und kann den Zugriff bei Bedarf auch jederzeit unterbrechen.

Komponente 6: Automation Terminalserver (ATS)

Dieser optionale Terminalserver auf Windowsbasis kommt zum Einsatz, wenn Tablet-Benutzer oder MAC-Benutzer einen Fernzugriff auf Anlagen, Steuerungen usw. benötigen. Dazu wird der Secure Access VPN (SAV) (siehe oben) auf dem Endgerät eingesetzt, darüber verbindet sich das Endgerät via RDP auf den Automation Terminalserver, der für die Benutzer ähnlich einem Jumpserver fungiert. Auf diesem Automation Terminalserver werden dann alle benötigten Windows-Applikationen für den Fernzugriff auf die Server/Maschinen/Steuerungen installiert.