zedas secure

Rechner ausschalten!

Ein Beitrag zu mehr Sicherheit bei Fernwartung

Ein ausgeschalteter Rechner gilt als sicher. Nur ist er leider zum Arbeiten nicht nutzbar.
Das Dilemma zwischen Funktion und Sicherheit beschäftigt jeden, der mit dem Thema IT-Schutz industrieller Anlagen in Berührung kommt. Alle Rechner, die eine Kommunikationsverbindung zu einer Produktionsanlage haben, sind ein potentielles Einfalltor und eine Gefährdung der IT-Sicherheit.

Slogans wie: „*Setze VPN-Router ein und du bist sicher!*“ suggerieren, dass mit dem Kauf und Einbau des Produktes IT-Sicherheit entsteht. In der Realität wird mittels „Fernwartung“ aber das Anlagen-Netzwerk, „sicher“ verschlüsselt über das Internet, mit dem Firmennetzwerk oder den Endgeräten des externen Dienstleisters verbunden.

Schutzbedarf

Fernwartung umfasst mehr schutzbedürftige Komponenten als nur das verbindende Netzwerk.

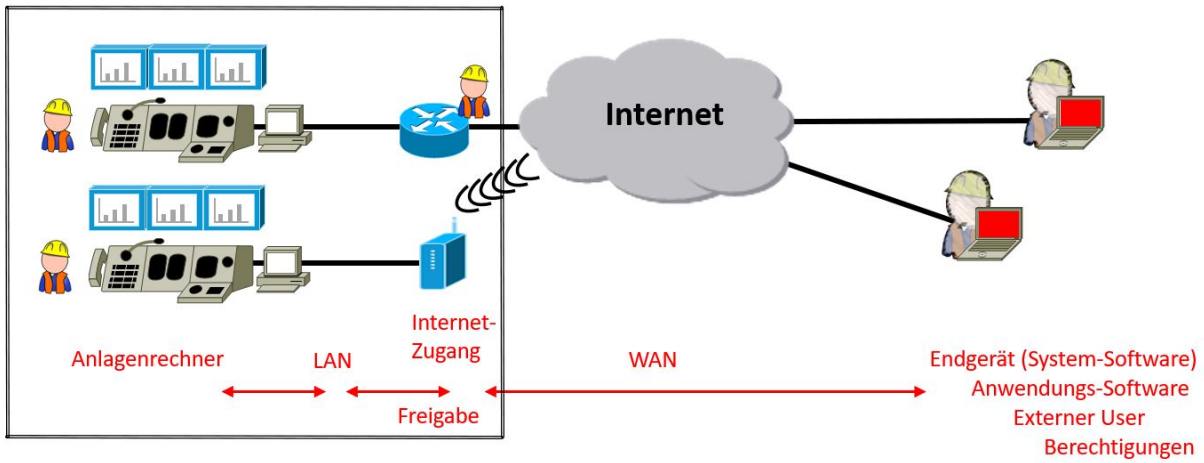

Abbildung 1: Schutzbedarf Fernwartung

Dazu gehören:

- Anlagenrechner (Zielsysteme)
- Lokales Netzwerk (LAN)
- Internetzugang (Verbindung von LAN und WAN)
- Weitverkehrsnetzwerk (WAN)
- Endgeräte (Servicerechner) inkl. Systemsoftware
- Anwendungssoftware für Zugriff auf Zielsysteme
- User-Accounts/Authentifizierung/Berechtigungen
- Freigabe und Kontrolle durch Produktionsverantwortliche
- System-Administration

Empfehlungen

Mit der IEC 62443, dem ICS Security Kompendium des BSI, dem VGB-Standard VGB-S-175 und dem Whitepaper des BDEW existieren mittlerweile Normen und Referenzarchitekturen, die eine gute Orientierung zum Thema IT-Sicherheit, speziell in Industriebereichen, geben.

Das BSI hat die grundlegenden Anforderungen an sichere Fernwartungszugänge im industriellen Umfeld [(Juli 2018; Gestaltung von Fernwartungszugängen [1])] unter den folgenden Punkten zusammengefasst:

- Architektur,
- sichere Kommunikation,
- Authentisierungsmechanismen,
- Organisatorische und
- Kundenspezifische Anforderungen

Der Abgleich der aufgeführten Normen und Standards mit den Angeboten des Marktes führt zur Erkenntnis, dass etablierte und praxiserprobte Standardprodukte verfügbar sind, die technische IT-Sicherheit mittels „defense in depth“ realisierbar machen. Dazu gehören Firewall-Systeme, VPN-Lösungen, starke Authentifizierung, Network Access Control, Virenschutz, Backup & Recovery, Intrusion Detection und Prevention, Fernsteuer-Software, bis hin zur Anomalie-Erkennung. Diese einzelnen Bausteine werden von verschiedenen Anbietern miteinander kombiniert und auch als dedizierte Fernwartungslösungen angeboten.

In vielen Fällen ist Fernwartung dieser Art fester Lieferbestandteil einer Anlage, was bisweilen beim Anlagen-Eigner zu einer großen Vielfalt von der Errichter-Lösungen führt.

Aus dem dringenden Bedarf nach Fernwartung resultieren zudem nicht selten einzelnstehende Lösungen, welche ein spezielles Anwenderproblem adressieren. Unberücksichtigt bleibt dabei die Integration der Fernwartung in ein übergreifendes IT-Sicherheitskonzept für Produktionsanlagen.

In Bezug auf IT-Sicherheit fokussieren aktuelle Fernwartungslösungen auf den Schutz des Anlagen-Netzwerkes und des Netzwerkzuganges. Firewall-Regelwerke bis auf Protokollebene, Verschlüsselung des Datenverkehrs und starke Authentifizierung sind charakteristisch. Die Endgeräte und die verwendete Software der externen Dienstleister bleiben jedoch außerhalb der Kontrolle des Eigners der Produktionsanlagen.

Ein weiteres Manko bei Nutzung marktüblicher Fernwartungslösungen besteht darin, dass die Fachsprache für industrielle Anwender unverständlich ist. Gespickt mit Anglizismen, Abkürzungen, Administratorrechten und Fachbegriffen der IT bleibt die sichere Anwendung ein Thema der IT-Abteilung, sofern vorhanden. Diese soll und kann, abseits vom eigentlichen Produktionsprozess, aber nicht die Prozess-Sicherheit verantworten.

Des Weiteren fehlen oft integrierte Organisationslösungen für den betrieblichen Einsatz, die ein zentrales und dezentrales Beobachten, Koordinieren und Kontrollieren von Fernwartungsarbeiten durch Mitarbeiter der Produktion gewähren. Von Team-Viewer, VNC oder VPN-Einwahl, nach außen vom Anlagenfahrer auf einem Steuerrechner der Anlage

freigeschalten, erlangt der Verantwortliche einer weiteren prozesstechnisch abhängigen Anlage keine Kenntnis. Er selbst kann derartige Software völlig unabhängig auf seinen Rechnern starten. Die Folgen in der Prozesskette sind nicht überschaubar. Eine übergreifende Koordination und Information zur Nutzung der Fernwartung ist nicht vorhanden.
Umgekehrt sollte bei zentraler Verwaltung der Fernwartungszugänge eine prozesstechnische Freigabe durch Anlagenverantwortliche erfolgen, damit nicht ohne ihr Wissen an der Anlage gearbeitet wird.

Angriffspunkt Endpoint

In den BSI-Veröffentlichungen zur Cyber-Sicherheit gehören zu den „Top 10 der Bedrohungen und Gegenmaßnahmen 2019 von Industrial Control Systemen“ [2]:

- das Einschleusen von Schadsoftware über **Wechseldatenträger und externe Hardware**,
- Infektionen mit **Schadsoftware über Internet und Intranet**,
- die Kompromittierung von **Extranet und Cloud-Komponenten** und
- der Einbruch über **Fernwartungszugänge**.

Allen vier Punkten gemeinsam ist, dass Angreifer mit ihrer externen Hard- und Software unzureichend gesicherte Netzwerkzugänge, interne Systeme und Software ausnutzen, um Schaden zu stiften.

„**Minimal need to know**“ gilt als ein wesentliches Lösungsprinzip des Problems. Einer Person stehen nur die Informationen zur Verfügung, die unmittelbar für die Erfüllung einer konkreten Aufgabe erforderlich sind. Das können Zugangsdaten, System- und Organisationswissen sein. Organisationsmängel, Social Engineering, menschliche Schwächen und unklare Definition der Aufgaben führen leicht zur Kompromittierung dieses Wissens. Deswegen ergänzt das Prinzip „**Minimal need to have**“ den IT-Schutz. Einer Person stehen dabei nur die Ressourcen und Systeme zur Verfügung, die unmittelbar für die Erfüllung einer konkreten Aufgabe notwendig sind. Eine Vielzahl von technischen Maßnahmen, wie verschlüsselte Übertragung von Daten per VPN, Firewall-Regelwerke, Zugriffsberechtigungen, Network Access Control, Härtung der Zielsysteme dienen der Umsetzung des Prinzips. Die Ausnutzung von Software-Schwachstellen, Denial of Service – Angriffe, Pishing, Brute Force Attacken und vor allem die unsichere Konfiguration von Systemen bieten jedoch auch hier zahlreiche Angriffsvektoren.

„Security by Default“ fasst die beiden Minimal-Prinzipien dahingehend zusammen, dass per Default alles verboten ist, was nicht explizit erlaubt wurde.

Konsequenterweise heißt das, dass **zum Zeitpunkt der Erfüllung einer konkreten Aufgabe** ausschließlich die dafür **notwendigen Hardware-, Software- und Netzwerk-Ressourcen** einem **berechtigten Anwender** zur Verfügung stehen dürfen.

Rechner und Software bei Externen, die z.B. per Fernwartung auf eine Anlage zugreifen, sind vom Anlageneigner allerdings kaum zu kontrollieren. Die Installation von Endpoint-Security-Software auf fremden Rechnern wird fast nie erlaubt. Die digitale Hoheit des Anlagen-Eigners endet zumeist vor den Fernwartungsrechnern seiner externen Dienstleister.

Endpoint-Security integriert

Aus den jahrelangen Erfahrungen der Integration eigener Software-Lösungen in Kundenumgebungen entwickelte die ZEDAS GmbH eine Lösung für industrielle Anlagen, die erprobte Sicherheitsverfahren mit einer außergewöhnlichen Staffelung in der Tiefe bei einfachster Handhabung kombiniert. zedas®secure gewährleistet dabei die durchgehende Umsetzung des Prinzips „Security by Default“ - auch auf den Endpoints, die von Externen für den Zugriff auf Produktionsanlagen benutzt werden.
Es ist eine standardisierte Lösung, die es einem produzierenden Unternehmen einfach und schnell ermöglicht, eine zentrale Lösung out-of-the-box für alle seine externen Service-Dienstleister zu etablieren.

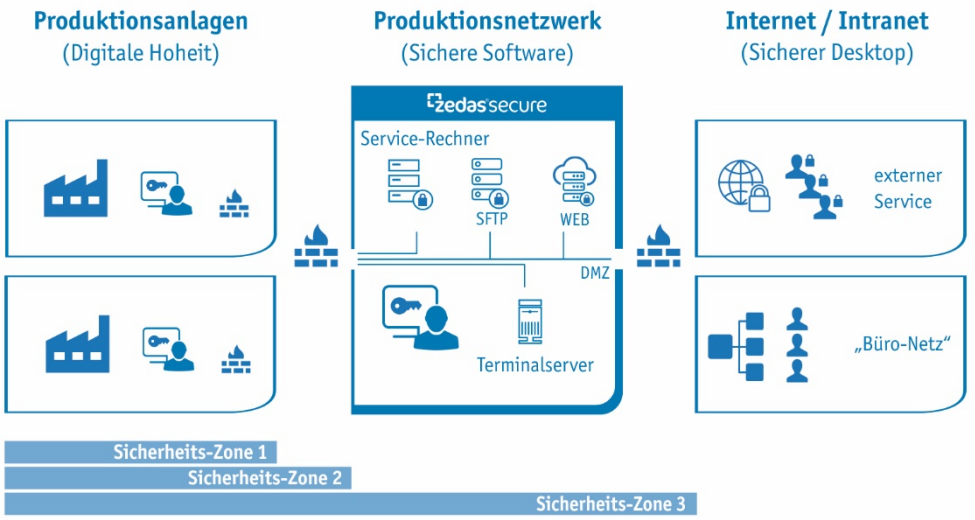

Abbildung 2: zedas®secure – herstellerübergreifendes Sicherheitskonzept im Überblick

Endgeräte, denen kontrollierter Zugriff auf Produktionsanlagen gewährt wird, sind in zedas®secure virtuelle Fernwartungsrechner, die sich in der Hoheit des Anlagenbetreibers befinden. Sie werden für jeden externen Dienstleister in dessen zugeordneter Demilitarisierter Zone (DMZ) aufgesetzt. Ihre Desktop-Oberfläche wird ausschließlich über Remote Desktop Protokoll und verschlüsseltes HTML5-VPN bereitgestellt. Dafür benötigt der externe Dienstleister lediglich einen HTML5-fähigen Browser. Die Installation eines VPN-Clients ist nicht erforderlich.

Der Netzwerkzugriff externer Dienstleister setzt eine starke Authentifizierung des Servicemitarbeiters mittels Token-Einmalpasswort voraus. Ein direkter Zugriff von Endgeräten der Dienstleiter auf Anlagen ist danach trotzdem nicht erlaubt. Das zweistufige Firewall-System gewährt Externen ausschließlich den Zugriff auf jeweils ihre virtuellen Fernwartungsrechner. Diese sind per Default **ausgeschalten**.
Technisch erzwungen, muss sich somit der externe Dienstleister telefonisch beim Anlagenbetreiber melden, um den Start seines Fernwartungsrechners anzufordern.
Mittels Software-App erfassen Schichtleiter die Fernwartungsanforderungen externer Dienstleister. Dazu gehören Namen der Firma und des Mitarbeiters, dessen Rückrufnummer, die Auftragsnummer, die Anlage mit Beschreibung der Servicetätigkeit, die Softwareanwendung sowie die voraussichtliche Dauer des Serviceeinsatzes. Dafür werden kaum mehr als 90 Sekunden benötigt. Alle einmal erfassten Eingaben werden wiederkehrend

zur Auswahl angeboten. Zudem bietet die App einen permanenten Überblick über alle inaktiven und aktiven Fernwartungsrechner.

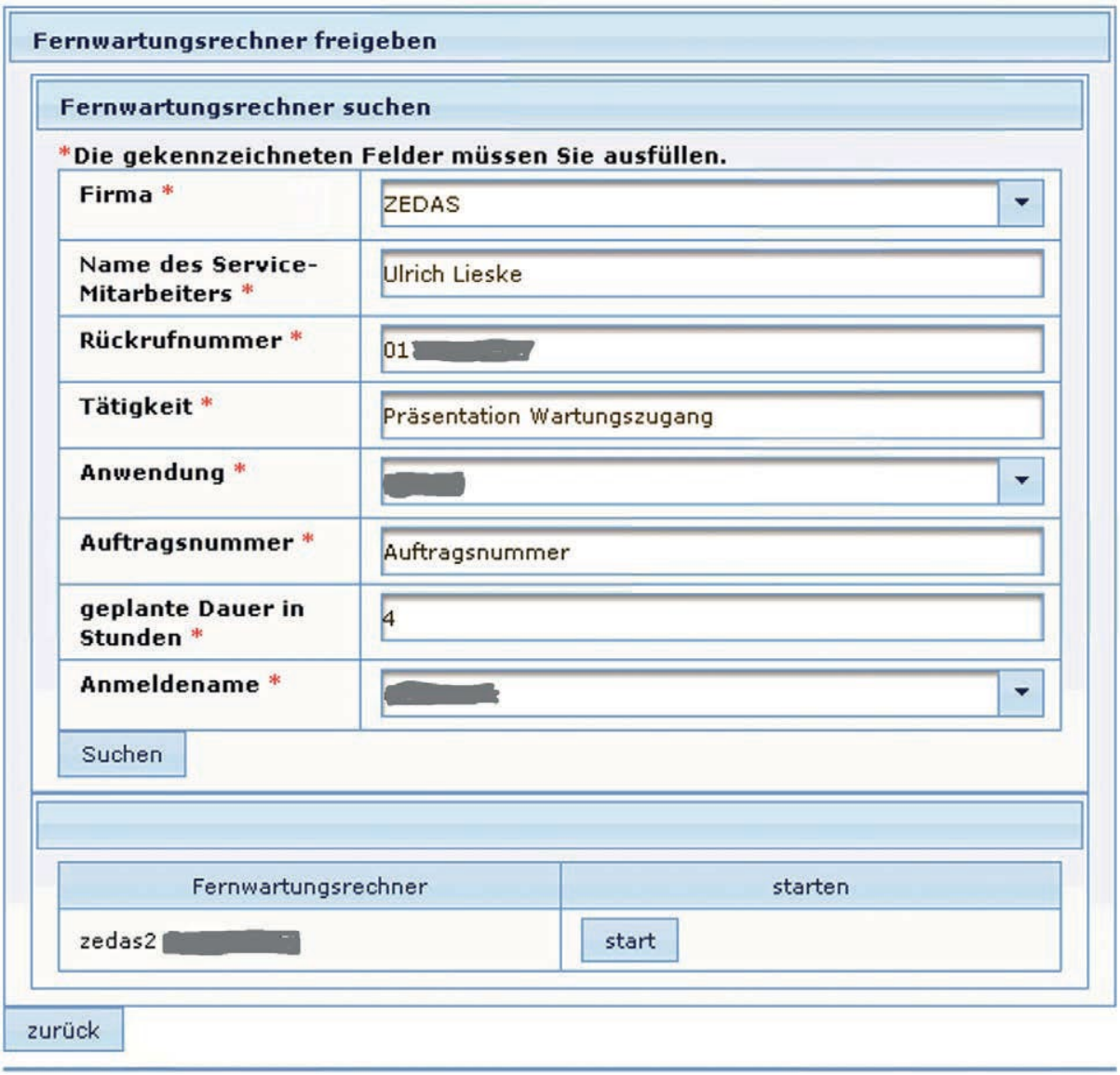

Abbildung 3: Erfassung Fernwartungsanforderung

Die genannten Informationen werden zusammen mit Start- und Abschaltzeit des virtuellen Fernwartungsrechners im Log-Buch elektronisch dokumentiert. Ihre Erfassung ist Voraussetzung dafür, dass der zugeordnete Fernwartungsrechner einfach aus der App heraus gestartet werden kann.

Nach dem Start eines Fernwartungsrechners befindet sich auf dessen stets leerer Desktop-Oberfläche lediglich ein Herunterfahren-Button. Der Rechtsklick ist deaktiviert. Es können keine Sondertasten, wie z. B. Windows-, Alt-, Steuerung- und F-Tasten, verwendet werden. Über den Start-Button sind keine weiteren Anwendungen sicht- oder startbar.

Im Zuge der Erfassung des Fernzugriffswunsches wird die Anlage bzw. das Zielsystem abgefragt, worauf der Zugriff erfolgen soll. Der Schichtleiter zaubert mit simplen Maus-Klicks ausschließlich die zugehörige Anwendungsverknüpfung auf den Desktop des externen Service-Partners. Nur diese kann er starten und verwenden.

Aktuelle Sessions auf den Fernwartungsrechnern lassen sich zudem auf administrativen Systemen spiegeln (Beobachten-Funktion), sodass ein Vier-Augen-Prinzip beim Fernzugriff möglich ist.

Ein weiteres Highlight ist die Absicherung der Serviceanwendungen über eine darunterliegende Anwendungsfirewall. Für jede installierte Serviceanwendung ist im Detail hinterlegt, welche Programme und Plug-Ins gestartet werden dürfen, welche Zielsysteme auf welchen Ports angesprochen werden dürfen und welche Parameter der Anwendung erlaubt sind.

Nach Abschluss des Fernzugriffs sind die Fernwartungsrechner heruntergefahren und ausgeschaltet. Die zugewiesenen Anwendungsberechtigungen werden automatisiert wieder zurückgenommen. Unabhängig davon hat der Schichtleiter in seiner App zu jeder Zeit die Option zur Zwangstrennung eines Fernwartungsrechners (Herunterfahren).

Fazit

Mit zedas®secure steht ein Fernwartungssystem als integraler Bestandteil eines weit gefassten IT-Schutzkonzeptes für industrielle Anlagen zur Verfügung. Es bietet Schutz auf Netzwerkebene, auf Endgeräte- und Software-Ebene sowie eine durch Produktionsmitarbeiter handhabbare Organisationsebene.

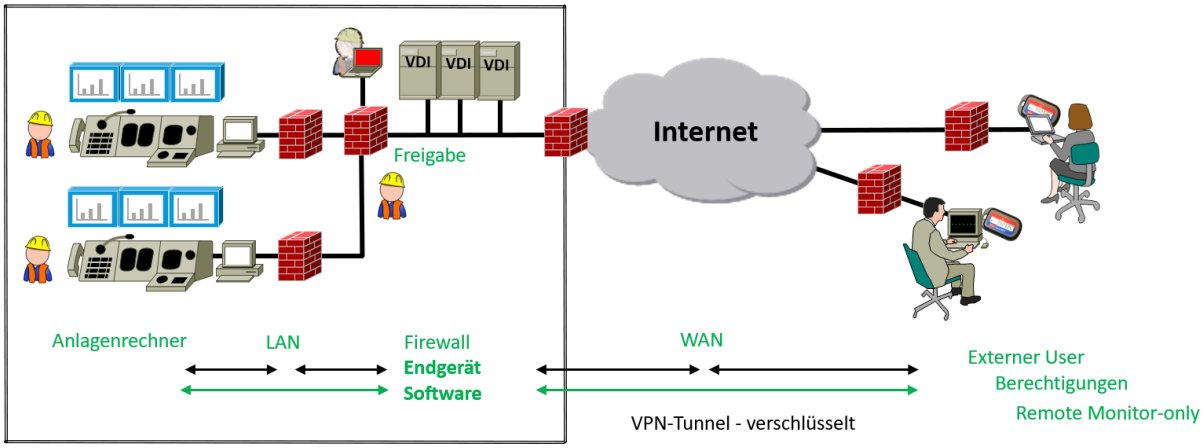

Abbildung 4: Umfassender Schutz der Produktionsanlagen bei Fernwartung

Das Prinzip „Minimal need to have“ wird konsequent auf die virtuellen Fernwartungsrechner und die darauf zu verwendende Software ausgeweitet. Der Anlagen-Eigner ist so in der Lage, seine digitale Hoheit auch über die Endgeräte des Anlagenzugriffs auszuüben. Mit der einfach handhabbaren Kontrolle über die virtuellen Fernwartungsrechner und Fernwartungsanwendungen durch Produktionsverantwortliche gelingt es IT-Sicherheit zu schaffen, die über die (noch) aktuellen Empfehlungen des BSI hinausreicht.

[1] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_108.pdf%3F__blob%3DpublicationFile%26v%3D3
[2] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile