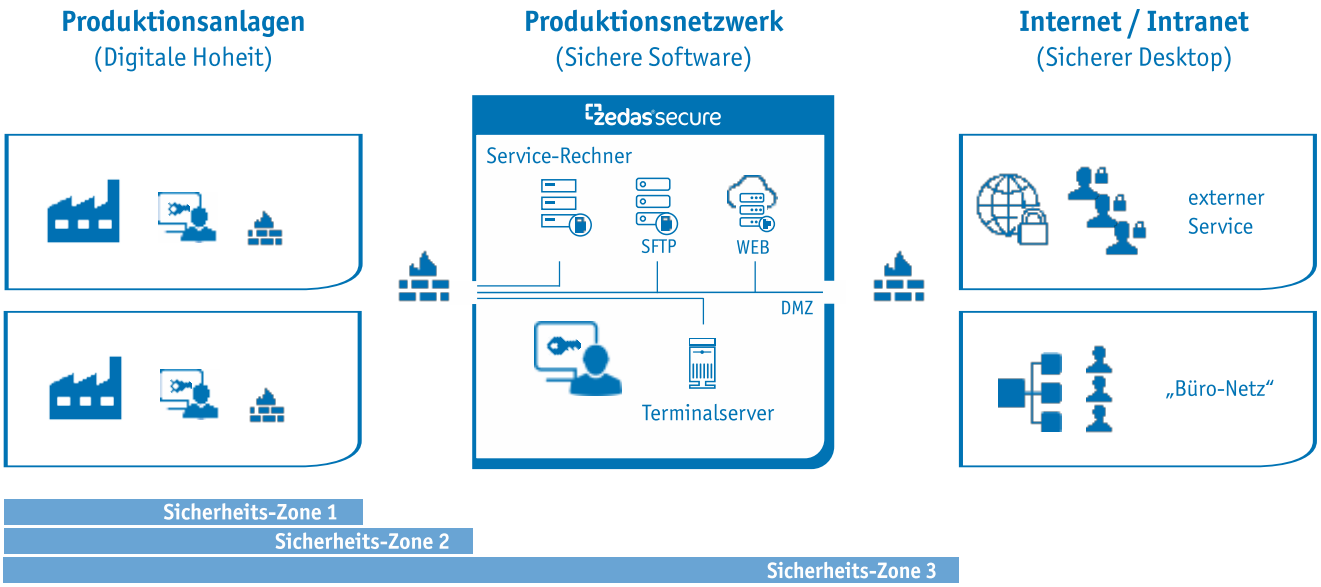
zedas®secure

Digitale Hoheit über kritische Infrastrukturen



zedas®secure - umfassendes Sicherheitskonzept im Überblick

Highlights

- Digitale Hoheit über Software, Netzwerk, Endgeräte und Daten
- Berücksichtigung der speziellen Anforderungen von Produktionsumgebungen
- Steuerung des digitalen Zugriffs durch Produktionsverantwortliche
- Einfache Betriebsführung und Handhabung
- Sichere Vernetzung von Anlagen und Systemen unterschiedlicher Hersteller und Lieferanten
- Verteidigung in der Tiefe durch Staffelung erprobter Sicherheitslösungen
- Integriertes Monitoring

Digitalisierung der Produktion sicher gestalten

Digitaler Zugriff und Datentransfer sind unerlässlich. Kaum ein Unternehmen verzichtet heute auf den Service für seine produzierenden Anlagen. Stillstand und Ausfall erzeugen rasch horrende Kosten. Dienstleister bieten Remote Services an, um schnellen und kostengünstigen Support für Anlagen bereitzustellen.

Mitarbeiter des eigenen Unternehmens benötigen Informationen direkt aus den Produktionsprozessen. Software-Systeme, innerhalb und außerhalb des Unternehmens, ziehen bzw. liefern Daten.

Es dauert nicht lange und die digitale Hoheit des Betreibers über seine Anlagen schwindet. Niemand weiß mehr sicher, wann, wie, wer von außen auf die Anlagen zugreift und welche Software dafür benutzt wird. Daten und Informationen fließen ab. Virenschutz und Security-Updates veralten. Die zunehmende Vernetzung der Produktionssysteme untereinander öffnet Tür und Tor für den möglichen Querzugriff zwischen den Anlagen und ihren Steuerungen.

Sichern Sie sich die digitale Hoheit über ihre Anlagen

zedas®secure ist ein umfassendes Sicherheitskonzept, speziell für kritische Infrastrukturen der Produktion. Auf Basis der konsequenten Umsetzung von Designkriterien hat es zum Ziel, dem Eigner der Anlagen die Kontrolle über Software, Hardware und Netzwerk zu gewährleisten und trotzdem die sichere Zusammenarbeit mit Lieferanten, Herstellern, Mitarbeitern, Kunden, Betreibern und Dienstleistern zu ermöglichen. Die technische Umsetzung ist standardisiert, praxiserprobt und skalierbar. Sie bietet alle Dienste und Funktionen, die für eine kollaborative Zusammenarbeit notwendig sind.

ZEDAS GMBH, A.-HENNECKE-STR. 37, 01968 SENFTENBERG

zedas®secure

Designkriterien für sichere Infrastruktur

Security by Design	Berücksichtigung von IT-Sicherheit/Datenschutz in der Planung
Security by Obscurity	Verschleierung, Beschränkung auf notwendige Informationen und Berechtigungen
Security by Default	Es wird/ist per Standard alles gesperrt, was nicht explizit erlaubt ist
Security by Himself	Jeder Mitarbeiter ist verantwortlich

Fernzugriff auf Anlagen – nicht ohne Freigabe

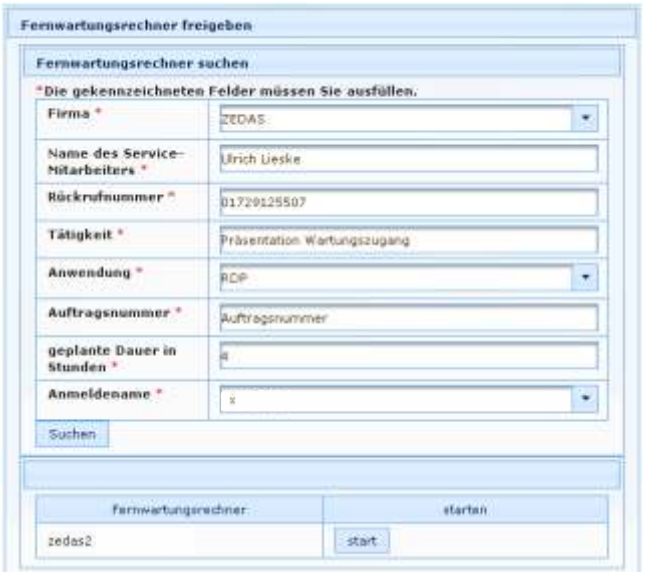
Die für jeden externen Dienstleister in einer dedizierten Sicherheitszone bereitgestellten virtuellen Rechner von zedas®secure sind im Grundzustand ausgeschaltet. Selbst mit erfolgreichem Netzzugang, nach starker Zwei-Faktor-Authentifizierung, sind die in den Firewall-Regeln freigeschalteten Zielsysteme nicht erreichbar. Damit wird technisch erzwungen, dass sich externe Dienstleister vor Beginn des Fernzugriffs (telefonisch) anmelden müssen.

In einer nutzerfreundlichen App erfasst etwa ein Schichtleiter zunächst Informationen zum gewünschten Fernzugriff und startet dann den zugeordneten Rechner per Mausklick. Dafür werden kaum mehr als 90 Sekunden benötigt. Zudem bietet die App einen permanenten Überblick über alle inaktiven und aktiven Servicerechner.

Software per Knopfdruck – das Highlight

Nach dem Start eines virtuellen Servicerechners befindet sich auf dessen gesicherter Desktop-Oberfläche lediglich ein Herunterfahren-Button. Im Zuge der Erfassung des Fernzugriffswunsches wird die Anlage bzw. das Zielsystem abgefragt, worauf der Zugriff erfolgen soll. Der Schichtleiter aktiviert per Mausklick die dafür erforderliche Anwendungsverknüpfung auf dem virtuellen Desktop des externen Service-Partners. Dieser nutzt die Anwendung ausschließlich über ein Remote Desktop-Protokoll.

Ein weiteres Highlight ist die Absicherung der Software auf dem virtuellen Service-Rechner 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 Servicerechner heruntergefahren und ausgeschaltet. Die zugewiesenen Anwendungsberechtigungen werden automatisiert wieder zurückgenommen.



App zum Starten des Fernwartungsrechners

zedas®secure – Schutz auf mehreren Ebenen

IT-Sicherheit in der Produktion bedarf neben technischer Lösungen auch eines adäquaten Sicherheitsmanagements. Aus den jahrelangen Erfahrungen der IT-Systemintegration in Produktionsbereichen entwickelte die ZEDAS GmbH ein Schutzschild, speziell für diesen Bereich. In der Praxis umgesetzt, verbindet es erprobte IT-Sicherheitsmechanismen mit einer außergewöhnlichen Staffelung der Verteidigung in der Tiefe bei einfachster Handhabung. zedas®secure bietet dabei umfassenden Schutz auf den Ebenen: Software, Hardware, Netzwerk und Organisation. Es ermöglicht einem produzierenden Unternehmen einfach und schnell, den sicheren digitalen Zugriff auf den Maschinenpark für eigene Mitarbeiter und alle externen Service-Dienstleister einheitlich zu etablieren.

April 2018

ZEDAS GMBH
ULRICH LIESKE
LEITER SYSTEMINTEGRATION
TEL.: + 49 (3573) 7075-15
ULIESKE@ZEDAS.COM
WWW.ZEDAS.COM