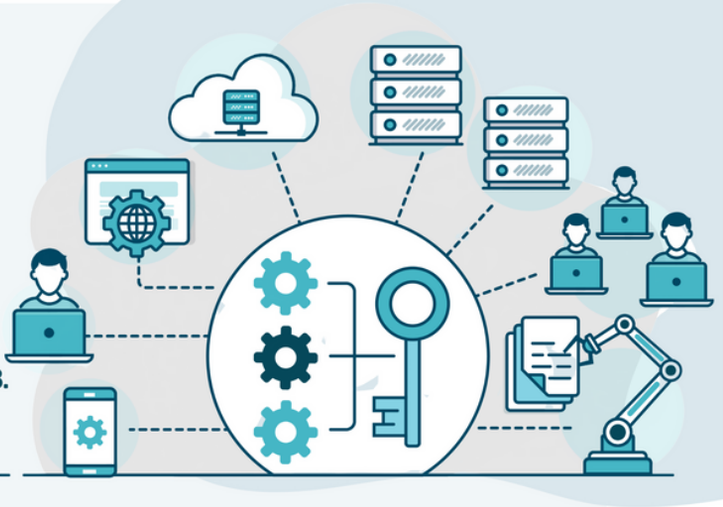
FERNZUGRIFFE EINFACH SCHÜTZEN - AUSFALL UND DATENABFLUSS VERHINDERN.



ERHÖHUNG DER CYBER-SICHERHEIT DURCH EINE ZENTRALE UND LÜCKENLOS DOKUMENTIERTE ZUGRIFFSMÖGLICHKEIT FÜR ALLE EXTERNEN DIENSTLEISTER UND PARTNER. MADE IN GERMANY SEIT 2003.

- ✓ KEINE ÄNDERUNGEN AN BESTEHENDEN IT-SYSTEMEN
- ✓ SICHERER UND DOKUMENTIERTER ZUGRIFF VON ÜBERALL - OHNE VPN
- ✓ OUT-OF-THE BOX - 1 TAG IMPLEMENTATION

Wer hat was wann wo und wie getan? Beantworten Sie es!

Top 5 Herausforderungen

Externe Dienstleister haben hohe Berechtigungen

Unkontrollierte Tätigkeiten und Spionage

Infektion mit Schadsoftware

Unklare Verantwortung bei Zwischenfällen

Fehlende Nachweise und Auditierbarkeit

VISULOX

Stellen Sie externen Dienstleistern nur die Rechte und Befugnisse bereit, die Sie zur Ausführung der beauftragten Arbeiten benötigen - **Just in Time**. Ihr Dienstleister erhält nur dediziert freigegebene Applikationen mit kontrollierten Möglichkeiten.

Stellen Sie externen Dienstleistern Zugriff nur per **Multi-Faktor-Authentifizierung** bereit und **zeichnen** Sie alle Eingaben, transferierte Informationen und Tätigkeiten **per Film auf**.

Trennen Sie Dienstleister logisch von sensiblen Daten. Stellen Sie eine kontrollierte Möglichkeit bereit, **Daten sicher und geprüft zu übertragen**. Verhindern Sie durch das Setzen von Regeln das Einschleusen von ungewünschter Malware.

Stellen Sie Ihren internen Mitarbeitern und externen Dienstleistern die Möglichkeit bereit in kritischen Situationen in einem **4-Augen-Prinzip** gemeinsam zu arbeiten und stellen Sie die Reproduzierbarkeit von Tätigkeiten sicher.

Greifen Sie jederzeit auf revisionssicher visuelle Nachweise zurück. Erfüllen sie g**esetzliche Compliance-Anforderungen** automatisch und rechtskonform.

Capterra 5

Teilnehmer der Allianz für Cyber-Sicherheit

amitego

Kontaktieren Sie uns | www.amitego.com

amitego AG
IM OBSTGARTEN 2B | CH-9602 WANGEN
TEL +41 79 699 92 00 | MOB +49 176 831 79 678

BSI Anforderung Fernwartung im Industrillen Umfeld (Stand 01. 2023)	VISULOX Remote Support
Architektur	
Einheitliche Lösung (kein Wildwuchs“): Besonders in größeren Infrastrukturen sollte möglichst eine einheitliche Lösung zum Einsatz kommen	Ein **zentraler unumgänglicher Zugang** zur IT- und OT Infrastruktur für alle externen Benutzer und Mitarbeiter Dritter und Partner
DMZ: Die Fernwartungskomponente sollte sich möglichst in einer vorgelagerten Zone (DMZ) befinden und nicht direkt im Produktionsnetz lokalisiert sein	Dedizierter Server als **zentrales Portal** in Form eines Fernwartungs-Gateway in der DMZ der Organisation
Granularität der Kommunikationsverbindungen: Der Fernwartungszugriff sollte möglichst nicht pauschal pro (Sub)Netz erfolgen.	Ferwartungs-Zugänge werden über das Portal direkt mit der Applikation / dem Endpoint gekoppelt und **individuell kontrolliert und dokumentiert**
Verbindungsaufbau: Der Fernzugriff sollte von innen aufgebaut werden oder von außen temporär begrenz werden	Zugänge können von außen nicht geöffnet werden. Fernwartung bspw. nur im **4-Augen-Prinzip** möglich.
Dedizierte Systeme: Die zur Fernwartung eingesetzten Komponenten sollten nur diesem Anwendungszweck dienen **Sichere Protokolle:** Es werden ausschließlich etablierte Protokolle wie IPsec, SSH oder SSL/TLS in aktuellen Versionen eingesetzt	Der Aufbau als gehärtete (virtuelle) **Appliance** garantiert die dedizierte Nutzung. Standardmäßige Integration von: SSH, SSL/TLS, RPD, xRDP, VNC, Telnet, x11, 3207, ...
Sichere Verfahren: Es werden hinreichend starke kryptographische Verfahren zur Verschlüsselung verwendet	Verschlüsselung durch kryptografische Verfahren gemäß **Stand der Technik** u.a AES 256
Authentisierungsmechanismen	
Granularität der Accounts: Es sollte nur ein Benutzer pro Account vorgesehen werden	Anbindung an User-Repositories u.a. Active Directory zur zentralen Admin aller Fernwartungszugänge. Verteilung der Rechte und "Least privileges"
Starke Authentisierungsmechanismen: Das beste Sicherheitsniveau bieten Zwei-Faktor-Verfahren	Standardmäßige Bereitstellung adaptiver **Multi-Faktor Authentifizierung** u.a. OTP, SMS, E-Mail, TicketID, Helpdesk
Angriffserkennung: Wünschenswert wären Mechanismen zur Detektion von Angriffen	Standardmäßige Erkennung von Fehlgeschlagenen Login-Versuchen und granulares **Event-logging und Reporting**
Organisatorische Anforderungen	
Risikoanalyse: Es erfolgt eine formale Risikoanalyse der konzipierten Lösung	Innerhalb des Migrationsprojekts abzubilden, aufbauend auf tiefgreifender Projekterfahrung
Minimalitätsprinzip: Es sind nur unbedingt erforderliche Fernzugriffsmöglichkeiten zu implementieren	Standardmäßige Bereitstellung adaptiver **Multi-Faktor Authentifizierung** u.a. OTP, SMS, E-Mail, TicketID, Helpdesk
Prozesse: Beim Betreiber der Anlage werden Prozesse etabliert u. a. Sperrung, Notfallzugang , Wechsel von Logindaten	Standardmäßige Erkennung von Fehlgeschlagenen Login-Versuchen und granulares **Event-logging und Reporting**
Inventarisierung: Sämtliche Fernzugriffsmöglichkeiten werden im Rahmen eines Sicherheitsmanagements erfasst	Aufgezeichnete Sessions generieren vielfältige Event-Logs. Diese können via gängiger **Log-Formate**, u. a. SysLog, an **SIEM / SOC** Systeme übersendet oder innerhalb des Systems verarbeitet werden
Zeitfenster: Remote-Zugänge werden nur bei Bedarf oder in einem definierten Wartungsfenster freigegeben	Die Freischaltung von Fernwartungszugängen folgt der **Prüfung festgelegter Kriterien**, u. a. Definition von Wartungsfenstern, erlaubte IP-Adressen, gültiges Ticket, Standort, MFA
Funktionsprüfung: Es erfolgt eine regelmäßige Prüfung der Funktionsfähigkeit der Fernwartung	Die Appliance beinhalten eine Keep-Alive Funktion, die einen Status zu jeder Zeit verfügbar macht und im Ernstfall Maßnahmen einleitet
Vorgaben für Fernwartende: Insbesondere im Falle der Fernwartung durch Dritte sind Vorgaben zu definieren	Die Vorgaben für externe Dritte können gruppenbasiert oder individuell festgelegt werden und folgen dem Ansatz, dass keine Benutzer anonym bleiben und nur die Berechtigungen erhalten, die Sie zu Ausführung Ihrer vereinbarten Tätigkeit benötigen
Patchprozess: Für funktionale Industriekomponenten	Ein zentrales Patch-Mangement stellt die funktionale Sicherheit von Industriekomponenten zu jeder Zeit sicher
Logging & Alerting: Es sind vorhandene Protokollierungsfunktionen zu nutzen	**Jeder Interaktion**, sowohl durch externe Dritte als auch interne Adminstratoren **erzeugt ein Event-log**. Eine lückenlose Protokollierung auf unterschiedlichen Ebenen ist durchgängig gegeben
Sonstiges	
Skalierbarkeit: Vorrangig in größeren Infrastrukturen können die Kosten für Betrieb, Wartung und Pflege durch ein zentrales Management, Bulk-Rollout, Bulk-Configuration oder Bulk-Actions, wie dem Ausführen von Skripten, stark gesenkt werden.	Es ist möglich komplexe **gleichartige Tätigkeiten in Workflows zu automatisieren** und u.a eine große Anzahl von Servern und Endpoints gleichzeitig aber kontrolliert zu administrieren
Investitionsschutz: Durch Berücksichtigung von möglichen zukünftigen Anforderungen wie beispielsweise der Unterstützung von IPv6 ist eine Auswahl von Produkten mit Blick auf Investitionsschutz und Nachhaltigkeit sinnvoll.	Die **Entwicklungsleistung wird seit über 20 Jahren in Deutschland erbracht** und orientiert sich am Stand der Technik und den individuellen Nachfragen der langjährigen Kundschaft. U. a. ist die Nutzung von IPv6 seit langer Zeit möglich.
Hochverfügbarkeit: Sofern entsprechende Anforderungen bestehen, sind Funktionen zur Umsetzung von HV-Konzepten	(Virtuelle) Appliance werden **redundant im Hot-Standy** aufgebaut. Je nach Anzahl von Nutzern und Zielsystemen über **Load Balancer** orchestriert