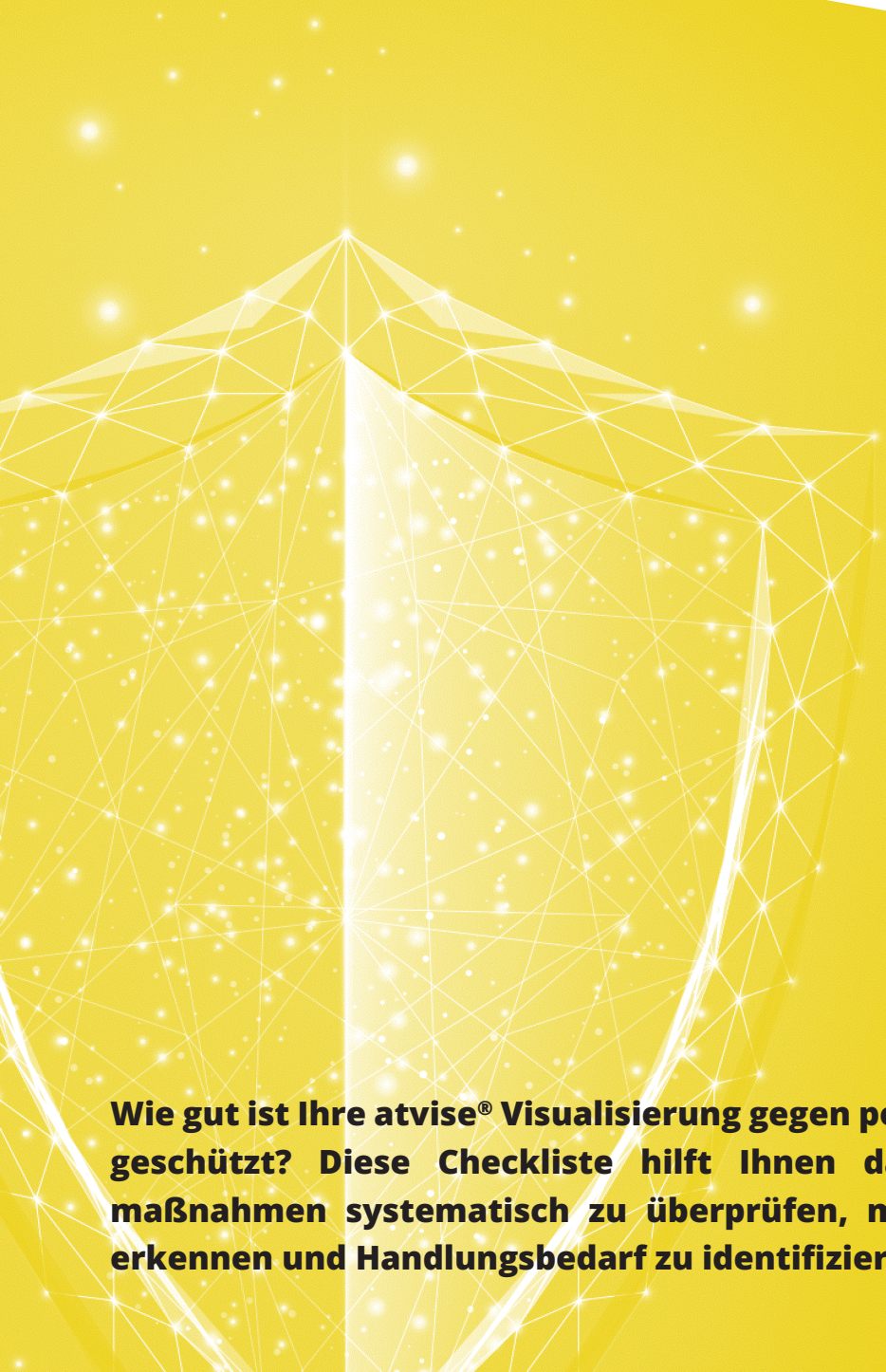
atvise® Security Check

für eine sichere und zuverlässige atvise® Visualisierung



Wie gut ist Ihre atvise® Visualisierung gegen potenzielle Sicherheitsrisiken geschützt? Diese Checkliste hilft Ihnen dabei, zentrale Sicherheitsmaßnahmen systematisch zu überprüfen, mögliche Schwachstellen zu erkennen und Handlungsbedarf zu identifizieren.

atvise® Security Check

Checkliste für eine sichere und zuverlässige Visualisierung

Prüfen Sie die folgenden Sicherheitsmaßnahmen für Ihre atvise® Installation. So behalten Sie den Überblick über Ihren Sicherheitsstatus und erkennen, wo noch Handlungsbedarf besteht.

Zugang & Berechtigungen

- ☐ Sichere Passwörter für alle Benutzer vergeben und die Passwortrichtlinie aktivieren.
- ☐ Die Zugriffskontrolle konsequent nutzen und Berechtigungen auf die jeweils erforderlichen Bereiche beschränken.
- ☐ Zwei-Faktor-Authentifizierung für kritische Zugänge einsetzen.

Verschlüsselung & Zertifikate

- ☐ HTTPS verwenden und unverschlüsselte HTTP-Verbindungen deaktivieren. Als Login-Methode „form“ oder „script“ verwenden.
- ☐ Offizielle Zertifikate einsetzen, Auto-Trust deaktivieren, Auto-Validate aktivieren und die Zertifikatslaufzeit auf maximal ein Jahr begrenzen und die Laufzeiten regelmäßig überwachen.
- ☐ Unverschlüsselte OPC-UA-Verbindungen unterbinden und Endpunkte sowie Datenquellen mit gültigen Zertifikaten absichern.
- ☐ In atvise® connect X gesicherte Protokollvarianten mit TLS verwenden, wo immer die Gegenstell sie unterstützt.

Netzwerk & Dateien

- ☐ Nur benötigte Netzwerkports freigeben und Engineering-Zugriffe von außen sperren.
- ☐ Verzeichnisse durch Betriebssystemrechte schützen und auf Netzwerkfreigaben verzichten.
- ☐ nodes.db und Archive verschlüsseln sowie den Zertifikatsstore und private Schlüssel zuverlässig schützen.

Betrieb & Datensicherung

- ☐ Für den Lizenzserver HTTPS verwenden, den Zugriff auf sein Installationsverzeichnis beschränken und Sicherungspfad sowie Sicherungszeitpunkt konfigurieren.
- ☐ Virenscanner-Ausnahmen für atserver.exe sowie das Installations- und Projektverzeichnis gemäß den atvise® Empfehlungen konfigurieren.
- ☐ Konsistente Backups erstellen, extern speichern und die Wiederherstellung regelmäßig testen.

Programmbibliotheken & Datenschutz

- ☐ Externe Programmbibliotheken nur nach sorgfältiger Prüfung ihrer Herkunft, Sicherheit und Aktualität einbinden.
- ☐ Bei der Verwendung von Benutzerkonten oder externer Authentifizierung sicherstellen, dass personenbezogene Daten durch geeignete Zugriffsrechte geschützt sind.

Hinweis: atvise® speichert in der Grundeinstellung keine personenbezogenen Daten. Werden Benutzerkonten angelegt oder externe Authentifizierung aktiviert, ist sicherzustellen, dass die Zugriffskontrolle auch diese Daten angemessen schützt.

Ergebnis des Security Checks vom .....

- ☐ Alle aufgeführten Maßnahmen sind umgesetzt.
- ☐ Einzelne Maßnahmen müssen noch überprüft oder umgesetzt werden.

Notizen / Offene Maßnahmen:

.....

.....

.....

.....

.....

.....

.....

.....

.....

Disclaimer:

- Diese Checkliste ersetzt keine vollständige Sicherheitsanalyse Ihrer Anlage.
- Alle Maßnahmen im Detail: atvise® Security Whitepaper
- Sicherheitslücke vermutet? Schreiben Sie an: visutec@bachmann.info
- Stand 10/2026

atvise®

www.atvise.com

atvise® Security Checklist
© 10/2026 by Bachmann Visutec GmbH