ISACA Switzerland Chapter

Nr. 02 | Juni 2024 | www.isaca.ch

NEWSLETTER

Management der IT- und Informationssicherheit
Eine wahre Flut an Methoden und Standards Seite @

TISAX 6 ist da – Anforderungen an die Automobilindustrie
Ein Überblick zur Anwendung von TISAX Seite @

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder Seite @

TISAX 6 ist da – Anforderungen an die Automobilindustrie

Von Andreas Wisler

TISAX (Trusted Information Security Assessment Exchange) ist ein Standard für Informationssicherheit, speziell entwickelt für die Automobilindustrie. Er basiert auf den Anforderungen des VDA ISA (Verband der Automobilindustrie Information Security Assessment), welcher wiederum auf dem internationalen Standard ISO/IEC 27001 aufbaut. Das Ziel von TISAX ist es, einen einheitlichen Sicherheitsstandard zu schaffen, um den Schutz und die Vertraulichkeit von sensiblen Informationen innerhalb der Lieferkette der Automobilindustrie sicherzustellen. Am 3. April 2024 wurde die Version 6.0.2 veröffentlicht. Der richtige Zeitpunkt, genauer in das umfassende Dokument zu schauen.

TISAX ermöglicht es Unternehmen, ihre Informationssicherheitsstandards durch eine externe, von der ENX Association akkreditierte Prüfstelle bewerten zu lassen. Die ENX Association agiert als Regulator und stellt sicher, dass alle akkreditierten Prüfstellen nach den gleichen Standards vorgehen. Die Ergebnisse der TISAX-Bewertung sind innerhalb des TISAX-Netzwerks austauschbar, was bedeutet, dass ein Unternehmen nicht mehrfach von verschiedenen Partnern geprüft werden muss.

Die Bewertung selbst umfasst verschiedene Aspekte der Informationssicherheit wie organisatorische Strukturen, physische und logische Zugangskontrollen, Umgang mit Daten und Datenschutz, Sicherheitsvorfälle sowie Geschäftskontinuitätsmanagement. TISAX legt auch besonderen Wert auf den Schutz von Prototypen und den Umgang mit vertraulichen Projekten.

TISAX Version 6 bringt einige Neuerungen und Verbesserungen gegenüber den vorherigen Versionen. Diese Aktualisierungen umfassen neue oder geänderte Anforderungen in Bereichen wie Cybersecurity, Datenschutz und IT-Compliance. Auf der Homepage von ENX (https://portal.enx.com/de-de/TISAX/) können in verschiedenen Sprachen das Teilnehmerhandbuch sowie der Fragebogen zur Prüfung der Informationssicherheit im Excel-Format heruntergeladen werden.

Teilnehmerhandbuch

Das «TISAX-Teilnehmerhandbuch» ist ein umfangreiches Dokument, das hilft, die TISAX-Anforderungen zu verstehen und zu erfüllen. Hier ist eine Zusammenfassung der wichtigsten Inhalte des Handbuchs:

1. Überblick und Zweck: Das Handbuch bietet einen Leitfaden für Unternehmen, um die Sicherheit ihrer Informationssysteme zu bewerten und sicher-

zustellen, dass diese den Standards von TISAX entsprechen. Es dient dazu, den von ihren Partnern geforderte Sicherheitsstandards nachzuweisen.

2. Geltungsbereich und Zielgruppe: Das Kapitel richtet sich an alle Unternehmen, die im TISAX-Prozess involviert sind, insbesondere an diejenigen, die ihre Informationssicherheitsmanagementsysteme gemäss den TISAX-Anforderungen überprüfen und zertifizieren lassen möchten.
3. Der TISAX-Prozess: Das Handbuch beschreibt detailliert die Schritte des TISAX-Prozesses, beginnend mit der Registrierung, der Durchführung der Sicherheitsbewertung (Prüfung) bis hin zum Austausch der Bewertungsergebnisse mit Partnern. Die Prüfung selbst läuft in vier Schritte ab: Vorbereitung, Prüfdienstleisterauswahl, Informationssicherheitsprüfung in drei Schritten (Kick-off-Meeting, Assessment-Phase 1 (Prüfer prüft das Self Assessment) und Assessment-Phase 2 (Prüfung vor Ort, teilweise auch Remote erlaubt)) sowie Prüfergebnis inkl. Erteilung des TISAX-Labels.
4. Registrierung und Prüfung: Die Schritte für die Registrierung im TISAX-Portal und die Vorbereitung auf die TISAX-Prüfung werden im Kapitel 4 erläutert. Unternehmen erfahren, wie sie ihre Systeme und Prozesse gemäss den TISAX-Standards evaluieren und entsprechende Sicherheitsmassnahmen implementieren können.
5. Ergebnisaustausch: Das Handbuch erklärt, wie zertifizierte Unternehmen ihre TISAX-Ergebnisse mit anderen TISAX-Teilnehmern teilen können. Dies ist besonders wichtig für Zulieferer, die ihre Sicherheitsstandards gegenüber Kunden im Automobilsektor nachweisen müssen.
6. Anhänge und zusätzliche Ressourcen: Dieses Kapitel bietet zusätzliche Ressourcen, Anhänge und Beispiele, die Unternehmen bei der Anwendung der im Handbuch beschriebenen Verfahren unterstützen.

Das Handbuch zielt somit darauf ab, den Unternehmen eine klare Anleitung zu geben, um den TISAX-Prozess erfolgreich zu durchlaufen und dabei effizient und konform zu den vorgegebenen Sicherheitsanforderungen zu arbeiten.

An dieser Stelle noch ein wichtiger Hinweis zum **Anwendungsbereich** (Scope). In ISO 27001 ist das Unternehmen frei, wie es diesen definiert. Anders bei TISAX. Folgender Standard Scope wird definiert: «Die Prüfung umfasst alle Prozesse, Verfahren und beteiligte Ressourcen, die unter der Verantwortung der zu prüfenden Organisation stehen und die für die Sicherheit der in den genannten Prüfzielen definierten Schutzobjekte und deren Schutzziele an den aufgeführten Standorten relevant sind. Die Prüfung wird mindestens im höchsten Assessment-Level durchgeführt, das in einem der aufgeführten Prüfziele gefordert ist. Alle in den aufgelisteten Prüfzielen geforderten Kriterien sind Gegenstand der Prüfung.»

Weiter gibt es klare Anforderungen an die **Prüfziele:** «Sie müssen Ihr(e) Prüfziel(e) während des Registrierungsprozesses definieren. Das Prüfziel (Assessment objective) bestimmt die maßgeblichen Anforderungen, die Ihr Informationssicherheitsmanagementsystem (ISMS) zu erfüllen hat. Das Prüfziel richtet sich ausschließlich nach der Art der Daten, die Sie im Auftrag Ihres Partners verarbeiten.» Zwölf Prüfziele sind im Handbuch abgebildet, inkl. Assessment-Level, die es einzuhalten gilt. Es handelt sich um Info high, Info very high, Confidential, Strictly confidential, High availability, Very high availability, Proto parts, Proto vehicles, Test vehicles, Proto events, Data, Special data).

Bei der Prüfung können fünf Arten von **Feststellungen** erfolgen:

- Hauptabweichung (erhebliches unmittelbares Risiko für die Informationssicherheit),
- Nebenabweichung,
- Beobachtung (Nichteinhaltung der Anforderungen oder der eigenen Richtlinien, die kein unmittelbares Risiko darstellt),
- Identifiziertes Verbesserungspotenzial sowie
- Konformität mit den Anforderungen.

Das ebenfalls zur Verfügung gestellte Excel-Dokument hilft dabei, das geforderte Self Assessment durchzuführen. Das Excel definiert im Register «Reifegrad» 6 Stufen: 0 – 5 (Unvollständig / Durchgeführt / Gesteuert / Etabliert / Vorhersagbar / Optimierend).

Weiter folgen Definitionen bevor die drei Teilgebiete Informationssicherheit, Prototypenschutz und Datenschutz folgen. Jede Anforderung enthält: Kontrollfrage, Ziel, Anforderungen (muss), Anforderungen (sollte), evtl. zusätzliche Anforderungen sowie den Verantwortlichen.

Im Register «Informationssicherheit» sind zusätzlich Verweise auf die ISO 27001 (Ausgabe 2013 und 2022), ISA/IEC 62443, NIST Cyber Security Framework 1.1 sowie Verweise auf Implementierungsanleitungen des BSI 200-2, dem Grundschutzkompendium sowie NIST SP800-53r5 enthalten.

Da TISAX ein anerkannter Standard in der Automobilindustrie ist, wird eine erfolgreiche Zertifizierung oft als wichtiger Wettbewerbsvorteil angesehen. Einige Automobilhersteller sind sogar dazu übergegangen, dies verbindlich von allen Zulieferern zu verlangen. Ohne Zertifizierung darf nicht mehr mit diesem Lieferanten gearbeitet werden. Dies stellt aktuell viele vor eine grosse Herausforderung, ist mit der Pflicht auch ein sehr kurzes Zeitfenster zur Umsetzung angesetzt worden.

Für die Automobilindustrie bietet TISAX somit nicht nur Sicherheit, sondern auch eine erhöhte Transparenz in Sicherheitsangelegenheiten. Es fördert eine Kultur der kontinuierlichen Verbesserung in der Informationssicherheit und hilft, die Resilienz gegenüber Cyberangriffen zu stärken. Durch die Teilnahme am TISAX-Netzwerk können Unternehmen auch von den Erfahrungen anderer lernen und Best Practices in der Branche teilen.

DER AUTOR

Andreas Wisler ist Inhaber der Firma goSecurity AG (https://goSecurity.ch). Er ist CISA, CDPSE, ISO 22301, 27001 sowie der erste Schweizer ISO 27701 Lead Auditor. Seit über 20 Jahren ist er im IT-Sicherheitsbereich tätig und unterstützt Firmen beim Aufbau eines ISMS und der Erlangung des ISO 27001 Zertifikats. Alle zwei Wochen veröffentlicht er den Podcast «Angriffslustig», zu abonnieren unter https://angriffslustig.ch.