audatis
Datenschutz und Informationssicherheit | CONSULTING

Whitepaper

TISAX[1] Standard zur Informationssicherheit

[1] TISAX ist eine eingetragene Marke der ENX Association.

Zusammenfassung

Eine Kette ist nur so stark wie ihr schwächstes Glied. Das gilt auch für Lieferketten in der Industrie. Bereits ein Dienstleister, der seine Informationssicherheitspflichten nicht ernst nimmt, kann dazu führen, dass Geschäftsgeheimnisse an die Öffentlichkeit dringen. Kaum eine Branche hat so komplexe Lieferketten wie die Automobilindustrie, daher ist es wenig verwunderlich, dass die Anforderungen in diesem Bereich stetig steigen und Dienstleister immer häufiger zur Einhaltung von Standards für Informationssicherheit verpflichtet werden. Das aktuell wichtigste Instrument zum Nachweis der Einhaltung ist der TISAX (Trusted Information Security Assessment Exchange) Standard. Vielen ist das TISAX Label und Sicherheitsstandards im Allgemeinen jedoch noch unbekannt und die Anforderungen von Auftraggebern können dementsprechend viele Fragen aufwerfen.

Problemstellung

Der TISAX Standard basiert auf dem VDA ISA Fragebogen, welcher wiederum stark an den ISO 27001 Standard angelehnt ist. Beide Standards zielen darauf ab, ein unternehmensinternes ISMS (Informationssicherheits-Management-System) zu etablieren, welches die Planung, Implementierung und Kontrolle von Sicherheitsmaßnahmen intern strukturiert.

Der TISAX Standard wurde ins Leben gerufen, um den Auditierungsprozess und das Sicherheitsniveau innerhalb der Automobilindustrie auf ein einheitliches Level zu bringen. Dabei wurde laut eigenen Angaben explizit darauf geachtet, den Auditierungsprozess möglichst effizient zu gestalten und Redundanzen zu vermeiden. Grundsätzlich können alle Dienstleister und Zulieferer innerhalb der Automobilindustrie von den Automobilherstellern zur Durchführung eines TISAX Assessments verpflichtet werden. Nach aktueller Lage ist davon auszugehen, dass mindestens 90% der Zulieferer innerhalb der nächsten Jahre dazu verpflichtet werden. An dieser Stelle sei erwähnt, dass dies nicht nur Zulieferer betrifft, welche Prototypen oder Steuergeräte herstellen. Bereits die Herstellung von unterstützenden Strukturen, wie z.B. Montagehilfen oder zunächst unsensibel erscheinenden Komponenten wie z.B. Autolack, kann indirekt zur Preisgabe von Geschäftsgeheimnissen führen. Zur Differenzierung können die Automobilhersteller ein bestimmtes Schutzniveau festlegen, so dass bestimmte Zulieferer weniger Aufwand betreiben müssen, die Anforderung eines TISAX Labels bleibt jedoch bestehen.

Das TISAX Audit muss von einer unabhängigen Stelle durchgeführt werden, jedoch gibt es keine Vorgaben bezüglich der vorgelagerten Planung und Implementierung der Sicherheitsmaßnahmen, d.h. grundsätzlich kann jedes Unternehmen ein Self-Assessment vornehmen und fehlende Maßnahmen intern im Alleingang umsetzen.[2]

Die Erfahrung und verfügbare Ressourcen im Bereich Informationssicherheit unterscheidet sich zum Teil erheblich zwischen mittelständischen Unternehmen. Ob eine Umsetzung im Alleingang der richtige Weg ist, muss jedes Unternehmen individuell entscheiden, aber wie kann diese Entscheidung getroffen werden?

---

[2] Der VDA ISA Fragebogen ist frei verfügbar unter der Adresse: https://www.vda.de/de/themen/sicherheit-und-standards/informationssicherheit/informationssicherheit-sicherheitsanforderungen.

Lösungsansatz

Konnte ein Unternehmen bereits Erfahrung im Bereich ISMS sammeln, z.B. durch eine bereits bestehende ISO 27001 Zertifizierung, empfehlen wir grundsätzlich dieses Vorgehen. Gibt es in diesem Bereich noch keine Erfahrung, kann eine Umsetzung im Alleingang sehr kostenintensiv und ineffizient sein. Die Weitergabe des Projekts "TISAX Audit" an die interne IT-Abteilung, ein Vorgehen, welches wir bereits sehr häufig in der Praxis beobachten konnten, führt in fast jedem Fall zu einem nicht-Bestehen des bezahlten Audits. Wird im Anschluss externe Hilfe hinzugezogen, muss das ISMS zumeist von Beginn an neu aufgebaut und strukturiert werden. Insgesamt können dabei somit sehr viel Ressourcen verschwendet werden.

Dies bedeutet jedoch nicht, dass ISMS-unerfahrene Unternehmen die Vorbereitungen vollständig auslagern sollten/können. Das Unternehmen muss interne Ressourcen und Kompetenzen im Bereich ISMS aufbauen, um das TISAX Audit zu bestehen. Der zentrale Ansprechpartner (häufig als Informationssicherheitsbeauftragter, kurz: ISB bezeichnet) sollte ein Mitarbeiter des Unternehmens sein und muss während des Audits zeigen, dass er sich über die internen Sicherheitsabläufe vollständig im Klaren ist.

Wir empfehlen daher eine interne Vorbereitung und Etablierung des ISMS mit externer Hilfe in Form eines ISMS-Beraters. Mithilfe des Beraters kann das Unternehmen ein ISMS effizient und kostengünstig implementieren und gleichzeitig Erfahrung sammeln, um das Management langfristig in die eigene Hand zu nehmen.

Autor und Ansprechpartner

Marcel Albrink
Consultant Informationssicherheit

Schwerpunkte: IT-Schwachstellenanalyse, Sichere Softwareentwicklung

Mail: m.albrink@audatis.de
Fon: 05221 87292-06
XING **Linkedin**

Haben Sie noch Fragen?

Wir haben versucht alle wichtigen Aspekte in unserem Whitepaper möglichst verständlich aufzubereiten.

Sollten Sie dennoch Fragen oder Beratungsbedarf haben, nehmen Sie gerne mit uns Kontakt auf.

Die audatis Consulting GmbH ist als Beratungsunternehmen auf die Bereiche Datenschutz und Informationssicherheit spezialisiert und betreut Kunden im In- und Ausland bereits seit 2011.

Neben der Stellung des externen Datenschutzbeauftragten begleiten und beraten wir Unternehmen, öffentliche Stellen und kirchliche Einrichtungen bei der Umsetzung des Datenschutzes, der Informationssicherheit und der Digitalisierung.

Als Teil der audatis Group hat die audatis Consulting GmbH Ihren Sitz im ostwestfälischen Herford und betreibt eine Niederlassung in Potsdam.

audatis Datenschutz und Informationssicherheit CONSULTING

audatis Consulting GmbH
Luisenstr. 1
32052 Herford
Deutschland

Fon: 05221 872 92-0
Fax: 05221 872 92-49

Mail: info@audatis.de
Web: www.audatis.de