TISAX – der Standard für Informationssicherheit in der Automobilbranche

Ein Beitrag von Daniel Wuhrmann

TISAX ist die Antwort der Automobilindustrie auf das wachsende Sicherheitsbedürfnis der Projektpartner im Umgang mit vertraulichen Informationen. Hierbei handelt es sich um einen Prüf- und Austauschmechanismus zur unternehmensübergreifenden Anerkennung von Assessments der Informationssicherheit in der Automobilbranche.

Im Jahre 2017 hat der Verband der deutschen Automobilindustrie (VDA) nach einem langjährigen Entwicklungsverfahren einen neuen Branchenstandard auf Grundlage der Norm ISO/IEC 27001 geschaffen.

TISAX: Trusted Information Security Assessment Exchange

TISAX soll umfassende Informationssicherheit für alle Stufen in der Lieferkette bieten, andererseits aber auch den Anerkennungsprozess externer Anbieter vereinfachen. Nach der zweijährigen Pilotierung in 2016 und 2017 führt spätestens seit 2018 auf mittlere Sicht kein Weg mehr am TISAX-Label vorbei, wenn man weiterhin mit oder für Automobilkonzerne tätig sein möchte. Betrieben wird TISAX von der ENX Association, einem Zusammenschluss europäischer Automobilhersteller, -zulieferer und -verbände, der vom VDA als neutrale Instanz beauftragt wurde.

Der TISAX-Prozess

Der gesamte TISAX-Prozess vollzieht sich in drei Schritten von der Registrierung über die eigentliche Prüfung bis hin zum Austausch der Prüfungsergebnisse.

Bei der TISAX-Registrierung ist besonders wichtig, dass die Prüf-Scopes sowie die Prüfziele festgelegt werden, da die eigentliche Prüfung im zweiten Schritt auf dieser Einordnung fußt. Im Rahmen der den Umfang festlegenden Prüf-Scopes ist zwischen Standard-Scope und (extended oder narrowed) Custom-Scope zu unterscheiden. Während nur die Prüfungsergebnisse, die aus den Standard-Scopes resultieren, von anderen TISAX-Teilnehmern (allgemeingültig) akzeptiert werden, ist ein narrowed Custom-Scope nicht TISAX-Label

geeignet und ein extended Custom-Scope nur im Rahmen der darin enthaltenen Standard-Scope-Prüfungsergebnisse. Neben dem Scope sind bei der Registrierung auch die Prüfziele festzulegen. Diese bestimmen die maßgeblichen Anforderungen an das Informationssicherheitsmanagementsystem (ISMS) des Teilnehmers und sind in Abhängigkeit von der Art der zu verarbeitenden Daten sowie deren Schutzniveau zu bestimmen. Prüfzielarten können dabei sein: Informationssicherheit, Prototypenschutz, Datenschutz sowie Schutz bei Anbindung Dritter, jeweils mit hohem oder sehr hohem Schutzbedarf. Je höher der Schutzbedarf hinsichtlich der einzelnen Daten ist, desto höher ist das Assessment-Level und desto höher ist die Prüfintensität, die von einer Selbstauskunft über Prüfung auf Aktenbasis bis hin zu einer Vor-Ort-Prüfung reichen kann.

Die eigentliche Prüfung in Schritt zwei beginnt mit einer VDA-ISA-Selbsteinschätzung des Teilnehmers (Prüfungsvorbereitung). Maßgeblich ist hier der entwickelte Fragenkatalog, dessen Bewertung durch ein Reifegrad-Modell (Level 0 – Level 5) umgesetzt wird.

Die Ergebnisse der Prüfung werden zusammengefasst und mit den zu erreichenden Zielreifegraden verglichen. Erst nach dieser Selbsteinschätzung wird ein von TISAX akkreditierter Prüfdienstleister ausgewählt, der die Informationssicherheitsprüfung(en) auf Grundlage der Prüf-Scopes und der angegebenen Selbsteinschätzung durchführt und kontrolliert. Diese Prüfung beginnt immer mit einer sog. Erstprüfung, die bei Konformität (d. h. Übereinstimmung von Anforderungen und tatsächlichem ISMS) direkt in einen offiziellen TISAX-Bericht und ein entsprechendes TISAX-Label mündet. Andernfalls, wenn das Ergebnis der Erstprüfung „hauptabweichend“ und nicht „konform“ ist, erstellt der Prüfdienstleister auf Grundlage der Erstprüfung einen Maßnahmenkatalog, dem nach Abarbeitung durch den Teilnehmer eine Nachprüfung folgt.

Maßnahmenplanung, -durchführung und Nachprüfung werden so oft wiederholt, bis der Teilnehmer die Anforderungen erfüllt und ein TISAX-Label ausgestellt bekommt oder aber die Maximalzeit von neun Monaten erreicht wird. Sollte innerhalb dieser neun Monate kein TISAX-Label ausgestellt worden sein, ist eine erneute Erstprüfung erforderlich.

Erhält der Teilnehmer ein TISAX-Label, werden seine Prüfungsergebnisse in einem letzten Schritt auf der Austauschplattform des ENX-Portals ausgetauscht, wobei grundsätzlich von einer Gültigkeit der TISAX-Label von drei Jahren, beginnend mit dem Zeitpunkt der Erstprüfung, ausgegangen werden kann.

Unternehmenskontakt: Melanie Schuh I Head of Marketing & Communications I T > +49 30 / 2332895 0 I E > melanie.schuh@reuschlaw.de