VDA-ISA und TISAX[1]-Modell

Im VDA (Verband der Automobilindustrie) existiert seit mehr als 10 Jahren der Arbeitskreis "Informationssicherheit". Dieser hat in mehreren Evolutionsstufen einen Fragenkatalog zur Informationssicherheit (ISA - Information Security Assessment) entwickelt, der sich auf wesentliche Aspekte der Internationalen Norm ISO/IEC 27001 abstützt. Seit Anfang 2017 ist der Katalog (VDA-ISA) in der Version 3.0 freigegeben und steht Interessierten zum Download unter

https://www.vda.de/de/themen/sicherheit-und-standards/informationssicherheit/informationssicherheit-sicherheitsanforderungen.html

zur Verfügung. Er hat sich in den vergangenen Jahren quasi zu einem Branchenstandard für Informationssicherheit entwickelt. Aktuell besteht er aus einem Basisbaustein sowie zusätzliche Module für Prototypenschutz, Anbindung Dritter (z. B. Projektbüros, Projektflächen) und Datenschutz (§11 BDSG zur Auftragsdatenverarbeitung), die in Prüfungen verwendet werden können. Weitere Module werden je nach Anforderung entwickelt und dem Katalog hinzugefügt.

Der VDA ISA Fragenkatalog wird von den Mitgliedsunternehmen sowohl für interne eigene Zwecke verwendet als auch für Prüfungen bei Lieferanten und Dienstleistern, die sensible Informationen aus den jeweiligen Häusern verarbeiten. Diese Prüfungen, insbesondere bei Dienstleistern und Lieferanten, wurden in der Vergangenheit häufig in Eigenregie des jeweiligen Unternehmens durchgeführt. Dies hatte zur Folge, dass ein Dienstleister bzw. Lieferant in mehr oder weniger kurzen Abständen mehrfach geprüft werden konnte. Die zuständigen VDA-Gremien haben inzwischen die inhaltlichen und formalen Voraussetzungen geschaffen, für das Information Security Assessment (ISA) einen gemeinsamen Prüf- und Austausch-mechanismus (TISAX) im Bereich Automotive und darüber hinaus zu etablieren, um diese Mehrfachprüfungen zu vermeiden. Das TISAX Modell wurde dabei so aufgebaut, dass es möglichst universell einsetzbar ist und damit ggf. auch weiteren Branchen offensteht.

Seit Mai 2016 ist das hierfür entwickelte Konzept in einer Pilotimplementierung erprobt worden. Der Betreiber des TISAX selbst ist die ENX[2] Association, die wiederum vom VDA als neutrale Instanz mit der Durchführung betraut wurde. Der TISAX ermöglicht Wettbewerb unter akkreditierten Prüfdienstleistern und ermöglicht durch die Standardisierung und Qualitätssicherung eine gemeinsame Anerkennung von Prüfergebnissen unter den TISAX Teilnehmern. Diese Prüfdienstleister prüfen auf Grundlage des gemeinsam im VDA verabschiedeten Fragenkatalogs.

TISAX Teilnehmer sind alle Unternehmen, die im TISAX Prüfungen anfordern bzw. Prüfergebnisse bereitstellen wollen. Hierbei gibt es zwei Rollen, die des Informations-empfängers „Information Consumer“ (fragt Prüfungsergebnis ab) und die des Teilnehmers „Information Contributor“ (liefert ein Prüfergebnis). Der „Information Contributor“ unterzieht sich auf Anforderung eines „Information Consumers“ einem Assessment oder lässt sich eigeninitiativ prüfen. Nach Durchführung des

[1] **T**rusted **I**nformation **S**ecurity **A**ssessment e**X**change
[2] **E**uropean **N**etwork e**X**change

Assessments durch einen akkreditierten Prüfdienstleister werden die Prüfergebnisse dem „Information Consumer“ als Anforderer zur Verfügung gestellt. Darüber hinaus kann das geprüfte Unternehmen auf Anfrage auch weiteren Teilnehmern im TISAX Prüfergebnisse in unterschiedlicher Detailtiefe verfügbar machen, wodurch zusätzliche Prüfungen durch andere mögliche „Information Consumer“ mit gleichen Sicherheitsanforderungen vermieden werden. Doppel- und Mehrfachprüfungen gehören damit der Vergangenheit an, was allen Beteiligten hilft, Zeit und Kosten zu sparen.

Die ENX Association agiert dabei als Governance-Organisation. Sie akkreditiert die Prüfdienstleister und überwacht die Qualität der Durchführung und der Assessment-Ergebnisse. Rechtlich wird diese Kontrollfunktion durch ein Vertragsdreieck abgesichert, welches sowohl aus einem Vertrag zwischen ENX und jedem akkreditierten Prüfdienstleister wie auch den Allgemeinen Geschäftsbedingungen (AGB) zwischen ENX und jedem Teilnehmer besteht. Der Teilnehmer stimmt diesen AGB durch die Registrierung zu. So kann sichergestellt werden, dass die Resultate am Ende einer gewünschten Qualität und Objektivität entsprechen sowie angemessene Rechte und Pflichten der Teilnehmer garantieren und damit auch den Anspruch der „Information Consumer“ Teilnehmer gerecht werden.

Für eine gegenseitige Anerkennung von Prüfungsergebnissen ist eine Registrierung als Teilnehmer im TISAX eine notwendige Voraussetzung. Um sich zu registrieren, müssen Sie ein Registrierungsformular ausfüllen, welches Sie bei der ENX Association unter der E-Mail Adresse **tisax@enx.com** oder telefonisch unter **+49 69 986692 777** anfordern können. Weitere Informationen finden Sie auch unter www.enx.com/tisax.