TISAX – Der Standard zur Informationssicherheit in der Automobilindustrie

Bedeutung von Informationssicherheit

„Augmented Reality“, „Künstliche Intelligenz“ oder „Internet der Dinge“, um nur drei Begriffe zu bemühen, sind heutzutage in aller Munde. Dabei stehen diese Begriffe stellvertretend für eine voranschreitende Digitalisierung, bei der die Unternehmen mal mehr, mal weniger aktiv werden, um ihre Rolle unter diesen neuen Rahmenbedingungen zu finden. Interessant dabei ist, wie vielfältig die Ausprägungen des Begriffes Digitalisierung verstanden werden. Verstehen manche Unternehmen darunter die Verknüpfung der vorhandenen Systeme in der Betriebsorganisation, verfolgen andere den Ansatz einer eigenständig lernenden und entscheidungsfähigen virtuellen Umgebung.

Was jedoch bei all den verschiedenen Ausprägungen den Konsens bildet, ist die Tatsache, dass eine zuvor nie gekannte Quantität und Qualität der Informationsverarbeitung existiert. Es stellt sich also die Frage, wie mit den veränderten Rahmenbedingungen, im Kern also der enormen Informationsflut, die sich aus der Digitalisierung bildet, umzugehen ist. Dabei hat Informationssicherheit ohne Zweifel eine besondere Bedeutung.

Informationssicherheits-Managementsysteme

Der Trend, der sich hier zeigt und gewissermaßen eine Antwort auf die zunehmende Verarbeitung von Informationen bietet, ist ein Zuwachs an Informationssicherheits-Managementsystemen (ISMS). Zu nennen ist hier die ISO 27001 als international anerkannte Norm. Informationssicherheits-Managementsysteme bieten den Unternehmen die Möglichkeit eines systematischen Überblicks über die vorhandenen Unternehmenswerte, wie z.B. Hardware, Software, oder Infrastrukturen und veranschaulichen die Chancen und Risiken, die mit den Unternehmenswerten (sogenannten Assets) verbunden sind. Die gelungene Umsetzung eines solchen Managementsystems kann also zum einen entscheidende Vorteile für das Unternehmen, wie zum Beispiel einen optimierten Datenfluss, mit sich bringen und zum anderen werden Spielregeln definiert, die vor allem in Bezug auf das Erreichen der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit das notwendige Maß an Sicherheit gewährleisten (s. Abb. 1).

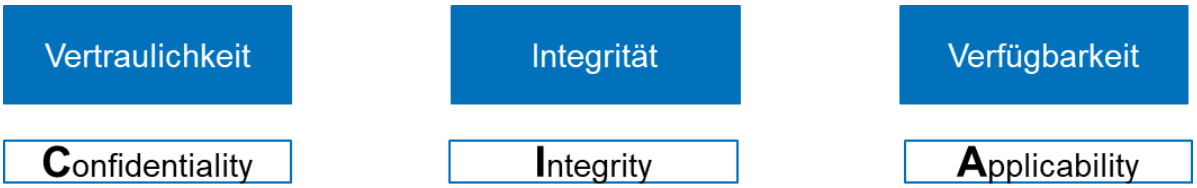

Abbildung 1: Schutzziele der Informationssicherheit

Kurzum bieten Informationssicherheits-Managementsysteme die Möglichkeit, die Informationen, die sich im Unternehmen befinden, systematisch zu managen. Durch eine Zertifizierung des entsprechenden Managementsystems haben Unternehmen zudem die Möglichkeit dies auch nach außen zu tragen um weiterhin Vertrauenswürdigkeit auszustrahlen.

TISAX als Standard der Automobilindustrie

Die Automobilindustrie ihrerseits hat ebenfalls die Zeichen der Zeit erkannt und den Standard namens Trusted Information Security Assemssment Exchange (TISAX) ins Leben gerufen. Das Ziel des Verbandes der Automobilindustrie (VDA) ist dabei einen auf die Automobilindustrie zugeschnittenen, ganzheitlichen Ansatz für ein gemeinsames und von allen anerkanntes Sicherheitsniveau zu etablieren. An dieser Stelle sei erwähnt, dass es bei Informationssicherheit immer um alle Informationen in einem Unternehmen geht und nicht nur um digitale Informationen. Somit bedeutet ein ganzheitlicher Ansatz neben technischer Sicherheit auch physische und organisatorische Sicherheit.

Entstanden sind die konkreten Anforderungen für TISAX aus einem von Sicherheitsexperten der Automobilindustrie entwickelten Anforderungskatalog (VDA Information Security Assessment) in Verbindung mit internationalen Standards wie der ISO 27001. Federführend bei der Entwicklung des gesamten Konzeptes ist dabei die ENX Association, die als neutrale Vereinigung der Automobilindustrie als Austauschplattform und Trägerorganisation von TISAX dient. Abbildung 2 veranschaulicht die Rollen bei dem Zertifizierungsverfahren, auch „ENX Triangle of Governance“ genannt.

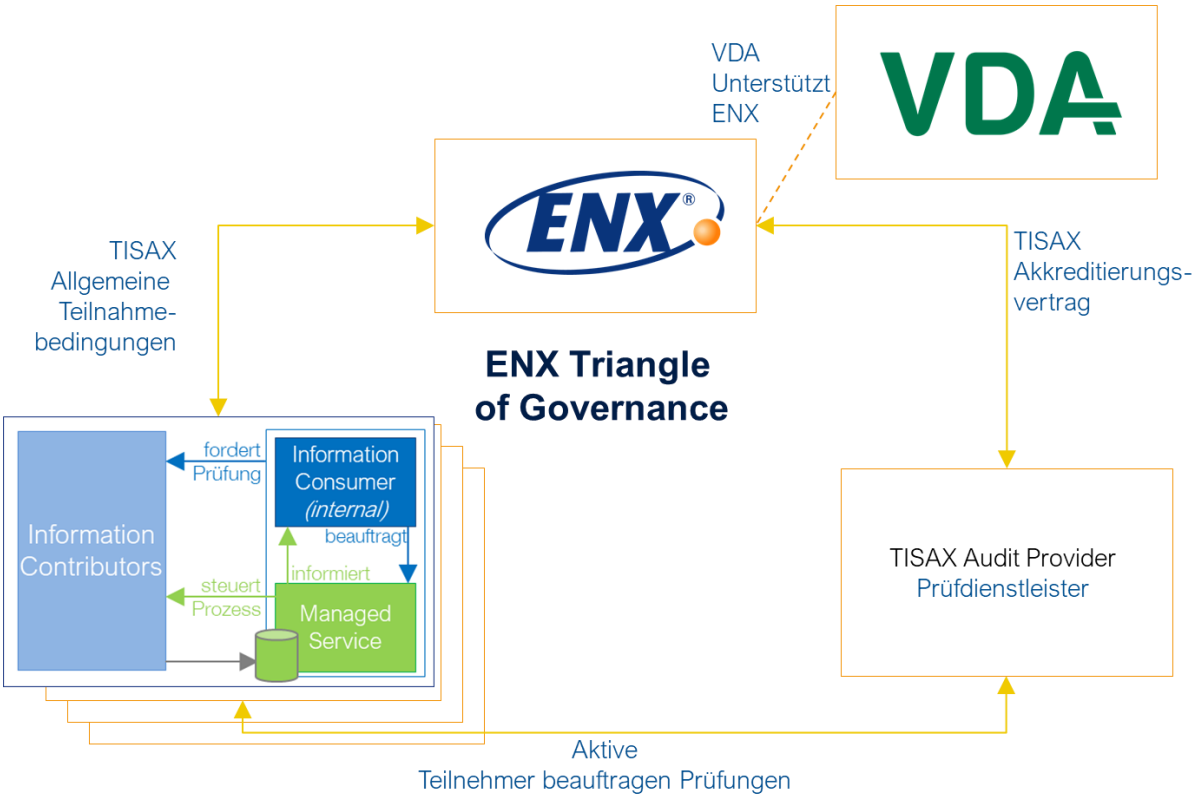

Abbildung 2: ENX Triangle of Governance

Quelle: ENX Association

Zunächst offen bleibt die Frage, warum die Automobilindustrie, abgesehen davon, dass die ENX Association ihren Standard auch auf andere Branchen ausweiten möchte, nun ihren eigenen Standard haben muss und sich nicht eines bereits vorhandenen Standards bedienen kann.

Wie bereits erwähnt, ist eines der Hauptziele von TISAX ein von allen anerkanntes Sicherheitsniveau zu etablieren. Entscheidend dafür ist, dass alle relevanten Prozesse in einem Unternehmen überprüft werden. Anders als beispielsweise bei der ISO 27001 kann man den Geltungsbereich, auch „Scope“ genannt, nicht frei wählen. Die Hürde zur Zertifizierung nach ISO 27001 war häufig die hohe Auditzeit und somit auch Kosten. Dies ist bei TISAX geringer. So stellt der „Standard-Scope“ von TISAX sicher, dass alle für den Kunden relevanten Prozesse geprüft werden. Die Beschreibung des „Standard-Scope“ lautet bei TISAX wie folgt (Gleich, Florian - TISAX-Teilnehmerhandbuch. Frankfurt-ENX Association, 2018):

„Der Standard-Scope erfasst alle Prozesse, Verfahren und beteiligte Ressourcen an den unten definierten Standorten mit denen Informationen verarbeitet werden, die Sicherheitsanforderungen von Partnern aus der Automobilindustrie unterliegen. Dies schließt sowohl die Erhebung, die Speicherung wie auch die Verarbeitung von Informationen ein. Beispiele für beteiligte Ressourcen: Arbeitsmittel, Mitarbeiter, IT-Systeme einschließlich Cloud-Diensten wie Infrastruktur/Plattform/Software als Service, physische Standorte, relevante Subunternehmer. Beispiele für Standorte: Bürostandorte, Entwicklungsstandorte, Produktionsstandorte, Rechenzentren.“

Nach außen wird eine erfolgreiche Prüfung über das TISAX Label kommuniziert. Dabei sorgt das ENX Portal, in dem auf Wunsch die eigenen Ergebnisse veröffentlicht werden können, für zusätzliche Transparenz.

Dass es sich bei TISAX um einen ausgereiften und sinnvollen Standard handelt, zeigen die aktuellen Zahlen der TISAX Teilnehmer. So verzeichnet die Automobilbranche nach zwei Jahren bereits 1800 Teilnehmer an 1500 geprüften Standorten. Besonders fällt dabei auf, dass nicht, wie man vielleicht vermuten würde, die großen Automobilzulieferer den Großteil der zertifizierten Unternehmen bilden, sondern mit 61% der Großteil der zertifizierten Organisationen Unternehmen mit weniger als 100 Mitarbeitern sind (s. Abb. 3).

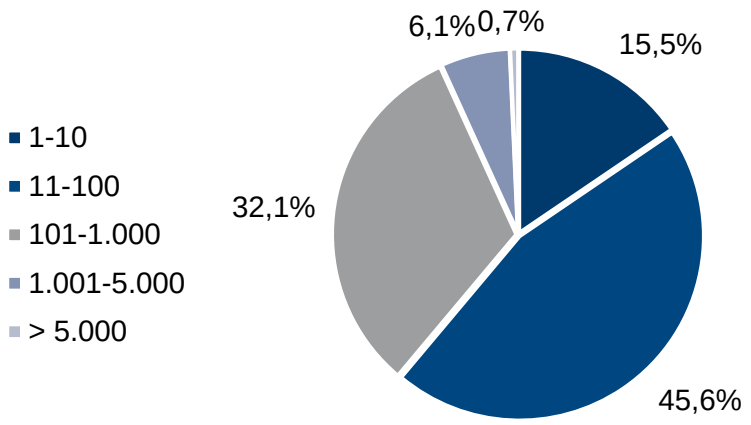

Abbildung 3: Anteil der zertifizierten Unternehmen je Anzahl Mitarbeiter

Quelle: ENX Association

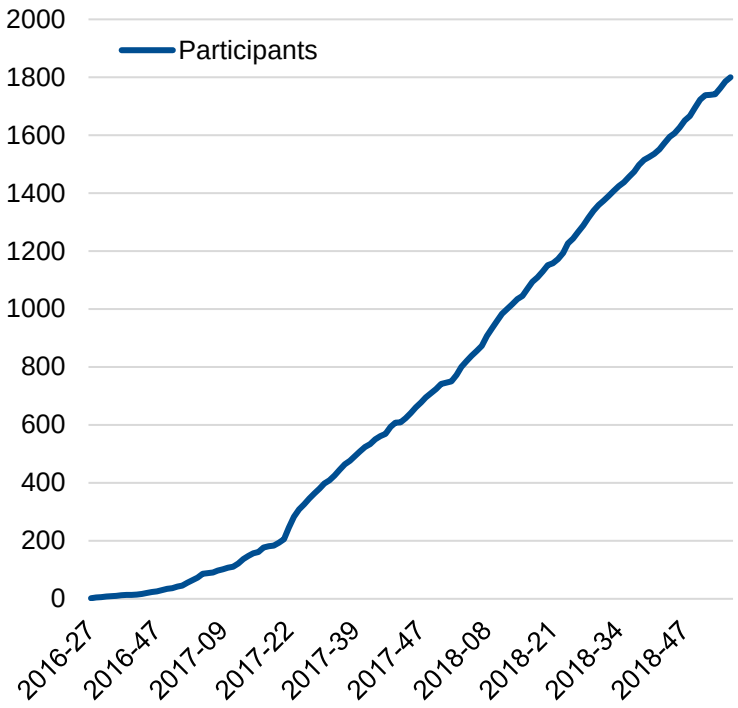

Abbildung 4: Teilnehmer TISAX

Quelle: ENX Association

Die Anzahl der zertifizierten Unternehmen wächst stetig weiter (s. Abb. 4), was mit Sicherheit auch daran liegt, dass der TISAX Standard bereits Teil der Kundenvereinbarung mancher OEM´s ist – weitere werden mit an Sicherheit grenzender Wahrscheinlichkeit folgen.

Aus vielerlei Hinsicht macht es also Sinn sich intensiv mit der Zertifizierung nach TISAX zu beschäftigen. Zum einen ist davon auszugehen, dass es verbreitet in den Kundenforderungen zu finden sein wird und zum anderen steigt der Druck bei zunehmender Anzahl an zertifizierten Marktbegleitern seine eigene Position durch ein solches Label zu legitimieren. Es kann also die Hypothese aufgestellt werden:

„Informationssicherheitsmanagement ist das neue Qualitätsmanagement“.

Jedoch auch abgesehen davon verlangt gerade die Digitalisierung eine gesteigerte Sorgfalt beim Umgang mit Informationen. Jedes Unternehmen sollte somit zeitnah die Chance nutzen, um nicht nur das notwendige Label nach außen zeigen zu können,

sondern tatsächlich das Management von Informationen strukturiert zu gestalten um somit einen echten Mehrwert für das Unternehmen zu erreichen.

Handlungsempfehlungen

Sofern Sie sich als Unternehmen in der Lieferkette der Automobilindustrie befinden, ist es ratsam für Sie, sofern noch nicht geschehen, sich intensiv mit TISAX auseinander zu setzten. Erste Anhaltspunkte dazu sind neben dem TISAX-Teilnehmerhandbuch Informationsveranstaltungen und kostenlose Erstberatungen, die durch die VIA Consult GmbH & Co. KG angeboten werden. Hier bekommen Sie einen ersten Überblick über den Ablauf des gesamten Zertifizierungsprozesses.

Sofern Sie nicht direkt zur Lieferkette der Automobilindustrie gehören, sorgen Sie trotzdem dafür, dass Sie zu den Unternehmen gehören, die sich frühzeitig mit dem Thema Informationssicherheit beschäftigt haben, denn es ist unbestreitbar, dass Informationssicherheit weiter an Bedeutung gewinnen wird. Die Zertifizierung nach einem Informationssicherheits-Managementsystem bildet vielleicht kein Alleinstellungsmerkmal, könnte Sie in Zukunft, sofern Sie keines haben, jedoch als potentiellen Lieferanten disqualifizieren. Zum Einstieg in die Thematik bietet die VIA Consult GmbH & Co. KG sogenannte Quick-Checks an, durch die das Unternehmen ohne großen Zeitaufwand Erkenntnisse darüber erlangen kann, wo es in Bezug auf die Anforderungen eines Informationssicherheits-Managementsystems steht. Dabei garantiert die jahrelange Erfahrung der VIA Consult einen pragmatischen Ansatz, der zum einen die Anforderungen an das System gewährleistet und zum anderen nur die notwendigen Ressourcen bindet.

Die Erfahrung zeigt auch, dass gerade kleine und mittelständische Unternehme bei der Suche nach einem Informationssicherheitsbeauftragten an ihre Grenzen stoßen. Tendenziell werden diese Themen sehr technisch betrachtet und fallen somit regelmäßig in den Verantwortungsbereich von IT- oder EDV-Leitern. Ähnlich wie beim Qualitätsmanagement, bei dem der Produktionsleiter die denkbar schlechteste Besetzung für den QMB ist, verhält es sich mit dem ISB und dem IT-Leiter. Bei einer Vielzahl von Maßnahmen sind es die organisatorischen und nicht die technischen Themen, die mit kleinstmöglichem (Kosten-) Aufwand den maximalen Nutzen erzielen. Hinzu kommt, dass sich eine Vielzahl der Problemstellungen aus den internen Gegebenheiten ergeben und der Prophet es in seiner Heimat nicht nur sprichwörtlich

am schwersten hat. Auch aus den genannten Gründen empfiehlt es externe Unterstützung einzuholen.

Für weitere Informationen und Fragen stehen wir Ihnen gerne zur Verfügung.

Karsten Kunde
Dipl.-Ing.
02761/83668-11
k.kunde@via-consult.de

Guido Solbach
Dipl.-Wirt.-Ing.
02761/83668-14
g.solbach@via-consult.de

Daniel Feldmann
M.Sc.
02761/83668-28
d.feldmann@via-consult.de