Schritt für Schritt zum Assessment

Informationssicherheit in der Automobilindustrie: Der Blick aufs Ganze

TEIL 1 Im Tisax-Verfahren wird die Informationssicherheit eines Unternehmens überprüft, anschließend werden die Ergebnisse in einem Report zusammengeführt. Die Prüfung schließt mit einem Label ab, das als „Eintrittskarte in die Automobilindustrie" gilt. Der Weg zum Label ist keine Kunst, aber sicherlich Arbeit.

Andreas Altena, Dr. Holger Grieb und Melanie Krauß

In dieser Ausgabe beginnt eine dreiteilige Beitragsserie zu Trusted Information Security Assessment Exchange (Tisax, eine eingetragene Marke der ENX-Association), dem branchenspezifischen Framework für Informationssicherheit in der Automobilindustrie. Erfahrene Experten beantworten grundsätzliche Fragen, die sich vielen Unternehmen auf dem Weg zum Assessment stellen, und geben praktische Empfehlungen (Bild 1).

Ist das Kunst oder kann das weg?

Schon seit Jahren finden sich Anforderungen und Regelungsvorgaben zum Thema Informationssicherheit in den Verträgen mit Ihren Kunden. Möglicherweise taucht der Begriff nicht explizit auf. Aber es werden z. B. die Themen Weitergabe der Unterlagen, Umgang mit Patenten und geistigem Eigentum, Anforderungen an beteiligte Mitarbeiter oder Weiterverwendung von erlangtem Know-how behandelt. Unter Umständen werden bereits Ausschlüsse formuliert, sodass Sie sich über den Kontrakt verpflichteten, im betreffenden Bereich nicht mit Mitbewerbern des Kunden zusammen zu arbeiten.

Sieht man mal davon ab, dass viele der Begriffe sich sprachlich geändert haben mögen, so ist doch festzuhalten, dass Ihr Unternehmen sich dazu entschieden hat, diese Regeln einzuhalten. Der formulierten Aussage, wonach immer mehr Regeln auf die Organisation zukommen würden, sodass die eigentliche Arbeit in den Hintergrund treten müsse, ist daher zumindest unter dem genannten Blickwinkel zu widersprechen. Die Regeln sind da.

Geändert hat sich zweifelsfrei aber die Bedeutung von Informationen und deren Schutzbedarf. Informationen werden nach wie vor in gedruckter Form, mündlich und digital ausgetauscht. Im Rahmen der allgegenwärtigen Digitalisierung sind Informationen schnell, zumeist unbedacht weitergeleitet, werden schützenswerte Informationen über das Mobiltelefon zu beinahe jeder Zeit und an beliebigen Orten übermittelt, wird eine technische Frage durch die Übersendung einer Konstruktionszeichnung quasi in „Echtzeit" beantwortet oder werden Projektbeteiligten und Lieferanten, weil einfach umsetzbar und zielführend, Daten- und damit Informationszugriffe gewährt.

Vor diesem Hintergrund und mit einigen negativen Erfahrungen im Gepäck verwundert es keineswegs, dass sich Kunden an die vertraglichen Vereinbarungen erinnern und die uns allen so bekannte Frage stellen: „Wie stellen Sie denn sicher, dass …?"

Dabei wird von Seiten der Unternehmen aus der Automobilindustrie auf das Tisax-Verfahren Bezug genommen. Dieses hat seinen Ursprung im „VDA ISA Standard zur Informationssicherheit", welchen ein Unternehmen unabhängig von seiner Größe erreichen muss, um als Zulieferer oder Dienstleister in dieser Branche fungieren zu können.

Es wäre doch wirklich mehr als peinlich, wenn wir nunmehr bekennen müssten, uns um diesen auch vertraglich vereinbarten Teil des Aufgabenkatalogs zur Informationssicherheit noch nicht so recht gekümmert zu haben. Anderseits macht es der nunmehr herangezogene Standard zwingend, sich damit auseinanderzusetzen und die bisher getroffenen Maßnahmen auf ihre Vollständigkeit und Wirksamkeit hin zu überprüfen. Diese Analyse sollte unternehmensintern durchgeführt und als Chance angesehen werden, die eigenen Informationswerte in den Schutz einzubeziehen.

Die Eingangsfrage ist damit beantwortet: „Es kann nicht weg!" und ist als eingegangene Verpflichtung anzusehen. Die Umsetzung ist keine Kunst, aber sicherlich Arbeit.

Empfehlung:
Legen Sie die vertraglich vereinbarten, die gesetzlich vorgegebenen sowie die innerhalb des Unternehmens gewünschten Regelungen zur Informationssicherheit übereinander und definieren Sie in Ihrem Unternehmen einen Standard, der die genannten Anforderungen umschließt. Darin liegt der wesentliche Vorteil eines einheitlichen Vorgehens gegenüber einer „mal dies und mal jenes"-Entscheidung. Aus diesem Standard leiten sich dann die erforderlichen Maßnahmen ab, um deren Einhaltung sicherzustellen.

ISMS und/oder Tisax?

Ein Informationssicherheitsmanagementsystem (ISMS) basiert auf einer internationalen Managementnorm [DIN ISO/IEC 27001:2017] und orientiert sich an den spezifischen Vorgaben Ihrer Organisation zum erforderlichen Schutz der (Informations-) Werte, also der Informationen von Wert (für Ihre Unternehmen). Das ISMS ist somit ein System von Verfahren und Regeln einer Organisation, die dazu die- »»»

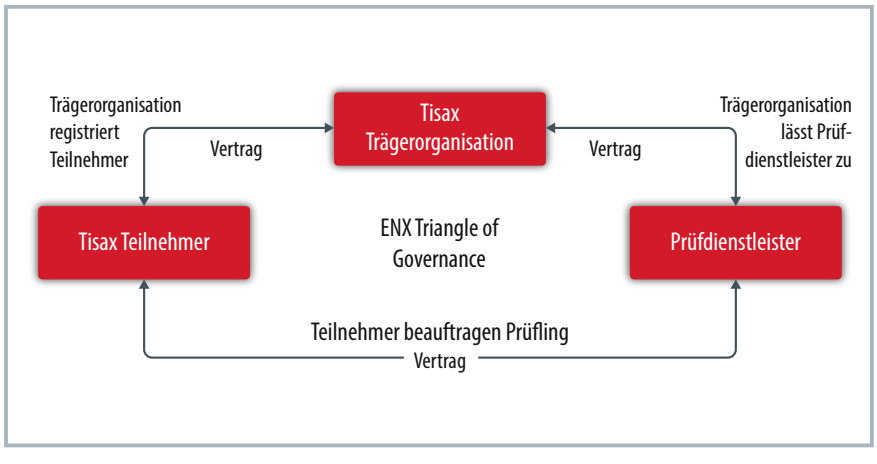

Bild 1. ENX – Triangle of Governance Quelle: DQS, ©Hanser

nen, die Informationssicherheit dauerhaft zu steuern und zu kontrollieren. Den „Informationen von Wert" werden ein oder mehrere Schutzziele zugeordnet (beispielsweise Vertraulichkeit, Integrität und Verfügbarkeit, aber auch Privacy oder Resilienz), welchen wiederum Maßnahmen zur Seite stehen, um etwaigen Bedrohungen oder Risiken angemessen und wirksam entgegen zu wirken.

Aufgrund seiner weitgehenden strukturellen Übereinstimmung zu bestehenden Managementsystemen, wie z. B. einem Qualitäts- oder Umweltmanagementsystem, ist ein ISMS gut zu integrieren. Existiert bereits eine prozessorientierte Ablauforganisation, so lassen sich die Anforderungen an den Schutz von Informationen prozessspezifisch gut identifizieren und implementieren. Das ISMS liefert dazu ein passendes Modell für die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und die Verbesserung des Schutzes von Informationswerten, um auf der Basis einer Risikoeinschätzung Unternehmensziele zu erreichen.

Die Risiken sind vor dem Hintergrund der Informationswerte zu behandeln, wobei der Maßnahmenkatalog so ausgestaltet werden muss, dass er die erkannten Risiken wirksam behandelt. Wie immer in Managementsystemen spielt die Angemessenheit der Maßnahmen eine entscheidende Rolle. Diese orientiert sich an dem (keineswegs nur monetären) Wert der Informationen in Verbindung mit einem zu akzeptierenden Restrisiko (auch als Risikoakzeptanzniveau bezeichnet). Ein ISMS ist anwendbar für jede Organisation jedweder Größe und branchenunabhängig.

Genau an diesem Punkt setzt Tisax (Trusted Information Security Assessment Exchange) an, das ein branchenspezifisches Framework für die Automobilindustrie bietet. Dienstleister und Zulieferer der Automobilindustrie müssen in dreijährigem Abstand nachweisen, dass sie die hohen Anforderungen ihrer Kunden hinsichtlich der Informationssicherheit einhalten.

Bisher wurden diese Prüfungen vor allem durch die Hersteller selbst durchgeführt. Basis dafür war ein vom Verband der Automobilindustrie (VDA) entwickelter Fragebogen zur Informationssicherheit (ISA – Information Security Assessment). Dieser bezieht sich auf wesentliche Aspekte der internationalen Norm ISO/IEC 27001 und ist um ein Reifegradmodell erweitert. Dieser Katalog war und ist auch zukünftig Basis für diese Prüfungen in seiner jeweils aktuellen Version.

Um wiederkehrende Prüfungen der unterschiedlichen Hersteller zu vermeiden, sieht das Tisax-Verfahren die unternehmensübergreifende Anerkennung von Assessments der Informationssicherheit auf der Basis eines gemeinsamen Prüf- und Austauschmechanismus vor. Die Ergebnisse bleiben dabei stets unter Kontrolle der Unternehmen, die sich prüfen lassen. Ein Austausch dieser Informationen erfolgt zudem nur nach Freigabe der Ergebnisse im Tisax-Netzwerk.

Die Ergebnisse dieser Prüfung haben eine Gültigkeit von drei Jahren und werden von allen ca. 600 Mitgliedern des VDA anerkannt. Die ENX Association (ENX-Verband), ein Zusammenschluss europäischer Automobilhersteller, -zulieferer und Verbände, fungiert dabei in dem System als vom VDA betraute Dachorganisation, welche die Prüfdienstleister zulässt und die Durchführungsqualität sowie die Ergebnisse der Assessments als neutrale Instanz überwacht. Nur durch Tisax zugelassene Prüfdienstleister dürfen diese Assessments durchführen. Die ENX-Tisax-Zulassung der Prüfdienstleister basiert auf einem Framework von Zulassungskriterien und Auditanforderungen (Accreditation Criteria and Audit Requirements, ENX Tisax Acar). Aktuell sind zwölf Prüfdienstleister durch die ENX zugelassen.

Empfehlung:
Unabhängig von den Anforderungen der Automobilhersteller hat die Auseinandersetzung mit der Informationssicherheit das Ziel, die sensiblen Informationen des eigenen Unternehmens wie auch die Ihrer Kunden systematisch und wirksam zu schützen.

Prüfen Sie daher über den Tisax-Standard hinaus die Anforderung an ein ISMS und deren Einbindung in die bestehenden Managementstrukturen, um die für Ihr Unternehmen erforderliche Ausrichtung und Wirkung zu erreichen. Das sichert Ihrem Unternehmen die entscheidenden Vorteile im Wettbewerb und zugleich eine nachhaltige Kundenbindung. ■

INFORMATION & SERVICE

BEITRAGSREIHE

Die dreiteilige Beitragsserie zu Trusted Information Security Assessment Exchange (Tisax), dem branchenspezifischen Framework für Informationssicherheit in der Automobilindustrie wird fortgesetzt.
Teil 2 „Verantwortliche und Beteiligte im Tisax-Verfahren" erscheint in QZ 8/2021 am 5. August 2021.
Teil 3 „Geltungsbereich und Dimensionierung des Assessments" erscheint in QZ 9/2021 am 2. September 2021.

AUTOREN

Andreas Altena ist Geschäftsführer der Sollence GmbH, Krefeld, Berater, Trainer und DQS-Excellence-Auditor mit den Kernkompetenzen Organisationsentwicklung und integrierte Managementsysteme, Qualitäts-, Informationssicherheits-, Risiko und (IT-)Servicemanagement.
Dr. Holger Grieb ist Lead-Consultant im Schwerpunkt Management & IT der Ksi Consult Ltd. & Co. KG, Düsseldorf, DQS-Auditor, DGQ-Prüfer, Lehrbeauftragter für „internationale Managementsysteme" an der Hochschule Fresenius, Düsseldorf.
Melanie Krauß ist Qualitätsmanagerin und leitende Auditmanagerin bei der Continental AG, Ingolstadt, Auditorin für Prozessaudits nach VDA 6.3 und Systemaudits nach IATF 16949, Sprecherin des DGQ-Fachkreises Audit und Assessment und DGQ-Regionalkreisleiterin Mittelbayern.

KONTAKT

André Säckel
DQS-Produktmanager u.a.
für ISO 27001 und Tisax
T 069 95427–8117
andre.saeckel@dqs.de