Gut vorbereitet für die Prüfung

Verantwortliche und Beteiligte im Tisax-Verfahren

TEIL 2 Im ersten Teil der Beitragsserie zu Tisax stand die grundsätzliche Berechtigung dieses Prüfverfahrens für Informationssicherheit in der Automobilindustrie im Vordergrund – und die hilfreiche Nähe zu ISO 27001. Heute lesen Sie, wer innerhalb und außerhalb des Unternehmens zur guten Vorbereitung und zum Gelingen des Assessments beitragen muss.

Andreas Altena, Dr. Holger Grieb und Melanie Krauß

Auf dem Weg zu Trusted Information Security Assessment Exchange (Tisax, eine eingetragene Marke der ENX-Association), dem branchenspezifischen Framework für Informationssicherheit in der Automobilindustrie, stellen sich den Unternehmen viele Fragen. Erfahrene Experten beantworten die wichtigsten und geben praktische Empfehlungen.

Ist das nicht nur eine reine IT-Aufgabe?

Oft wird Informationssicherheit mit IT-Sicherheit auf eine Stufe gestellt. Bei einer genaueren Betrachtung zeigt sich aber der Trugschluss. Betrachtet die Informationssicherheit in Gänze den Schutzbedarf von Informationen in einem Unternehmen, bezieht sich die IT-Sicherheit auf die rein technische Sicherheit in informationsverarbeitenden Anlagen (z. B. Computern).

Wie bereits im ersten Teil dieser Serie dargelegt, geht es bei der Informationssicherheit um die ganzheitliche Betrachtung von wichtigen und relevanten Informationen in einem Unternehmen.

Die erste Frage muss daher lauten: „Was ist für uns von Wert und darum auch schützenswert?“ Die Antwort kann, je nach Unternehmen und Branche, völlig unterschiedlich ausfallen. Für einen Softwarehersteller kann dies beispielsweise der Quellcode der Software sein, der auf keinen Fall in falsche Hände geraten darf. Für andere Unternehmen sind es Informationen zum Design des Produktes oder auch der technischen Spezifikationen bis zur Veröffentlichung. Für wieder andere Unternehmen geht es um Rezepturen, Fertigungs-

prozesse oder weiteres Wissen, das die Zukunftsfähigkeit des Unternehmens sicherstellen soll (Schlagwort: Was gehört alles zu einer Innovation?).

Innerhalb des Unternehmens können es auch durchaus bereichsspezifische Informationen sein, wie z. B. eine Personalakte. An letzterem Beispiel soll vor allem noch mal deutlich werden, dass die Informationssicherheit auch alle relevanten gesetzlichen und behördlichen Anforderungen mitberücksichtigt, hier z. B. die Datenschutzgrundverordnung und weitere zugehörige gesetzliche Regelungen.

Um all diese Anforderungen zu erfüllen, sind in Zeiten der Digitalisierung und der digitalen Transformation vor allem die elektronischen Daten von immer größer werdender Bedeutung und Wert. Viele Informationen (z. B. zu neuen Produkten und damit auch zu Prototypen) werden elektronisch gespeichert und verteilt.

Als ein entscheidender Bestandteil der Anforderungen zur Informationssicherheit setzt hier die IT-Sicherheit an und fordert einen Stand der Technik, um z. B. eine sichere IT-Infrastruktur (von einer Firewall über das Netzwerk bis zu den Endgeräten) zur Verfügung zu stellen. Dazu zählen Themen wie eine Authentifizierung von Benutzern über mehrere Faktoren (d.h. mehr als nur eine Kennung und ein Passwort), der richtige Einsatz von Verschlüsselungen in der Speicherung und Kommunikation oder Vorgaben zur Nutzung von Endgeräten („don't bring your own device", verbotene Apps und Programme) und der Segmentierung von Netzwerken.

Die dafür erforderlichen technischen und organisatorischen Anforderungen sind im VDA-ISA Fragenkatalog definiert und auch mit beispielhaften Kennzahlen zur Messung und Überprüfung dargestellt.

Unsere Empfehlung

Es steht außer Frage, dass Informationssicherheit die Zielsetzungen der Prozesse verändert. So wird beispielsweise bei dem Prozess „IT betreiben und aufrechterhalten" das Ziel von „Anwender sollen reibungslos arbeiten können" zu „nur autorisierte Anwender sollen unter definierten Bedingungen sicher arbeiten können". Dies greift in die Komfortzonen aller Beteiligten ein und ist als Veränderungsprozess anzusehen. Reaktionen wie: „So kann ich nicht arbeiten, hier muss die IT …" ist mit einem klaren Bekenntnis entgegenzutreten: „So wollen wir arbeiten, um die Daten von Wert zu schützen und die IT unterstützt uns darin!"

Kann ich das alles an die Leitung delegieren?

Auf den ersten Blick ist Informationssicherheit eine Aufgabe der obersten Leitung.

- Informationssicherheit und damit auch die Tisax-Anforderungen zielen eindeutig auf eine Gefahrenabwehr, also auf das Abwenden, Vermeiden und Abschwächen von Risiken.
- Im Verlaufe der Bestimmung von Maßnahmen, welche geeignet erscheinen, die Einhaltung der vorgegebenen Schutzziele sicherzustellen, kann es sich zudem als notwendig erweisen, bestimmte Risiken zu akzeptieren. Eine derartige Risikoakzeptanz erscheint beispielsweise sehr nachvollziehbar, wenn die Maßnahme zu aufwendig in Relation zum Informationswert erscheint.
- Die zu betrachtenden Risiken sind zudem vor dem Hintergrund der unternehmensspezifisch bestimmten Informationswerte und deren Schutzziele zu sehen.

Kaum eine oberste Leitung wird feststellen können oder wollen, dass diese Facetten der Gefahreneinschätzung und -abwehr nicht originäre Aufgaben der Leitung sind. Der zweite Blick sollte den bereits bestehenden Regelungen und Vorgehen gelten.

Kein Unternehmen steht hier vor dem Nichts. Ob bereits im Rahmen implementierter Managementsysteme (hier ist auf die Lenkungen von dokumentierten Informationen zu verweisen), bei der Umsetzung gesetzlicher Vorgaben wie dem Datenschutz (bspw. dem Umgang mit personenbezogenen Daten), bei Berücksichtigung von unternehmensinternen Vorgaben oder der Erfüllung von Kundenanforderungen – in allen Fällen kann, muss und sollte auf Bestehendem aufgesetzt werden. Da diese Themen eher in der Hand von Beauftragten für Managementsysteme, Datenschutz, Compliance oder von Projekt- und IT-Sicherheits-Verantwortlichen liegen, schauen wir hier nicht auf die oberste Leitung.

Die operative Umsetzung obliegt wiederum Allen im Unternehmen. Informationssicherheit wird nicht selten als Einschränkung empfunden und greift erfahrungsgemäß in die Komfortzonen aller Beteiligten ein. Der erforderliche Veränderungsprozess ist aktiv zu begleiten und zu unterstützen. Dies gilt unabhängig von der Entscheidung, die Tisax-Anforderungen umzusetzen und/oder ein Informationssicherheitsmanagementsystem aufzubauen.

Unsere Empfehlung

Die Ausrichtung der Informationssicherheit gibt zweifelsfrei die oberste Leitung vor. Die Ausgestaltung sollte auf Bestehendem aufsetzen und in der operativen Umsetzung alle im Unternehmen einbeziehen. Dabei kommt der Schaffung eines Bewusstseins für die zwingende Notwendigkeit der Informationssicherheit eine besondere Bedeutung zu. Jeder sollte sich der Risiken für die Informationswerte bewusst sein, aber auch die Chancen in der wirksamen Umsetzung der beschlossenen Maßnahmen sehen. Nur so kann eine Organisation sich auf Angriffe der Informationswerte (angemessen) vorbereitet zeigen.

Tisax zieht zwingend Kreise – und keineswegs nur runde?

Die Systematik ist ebenso bekannt »»

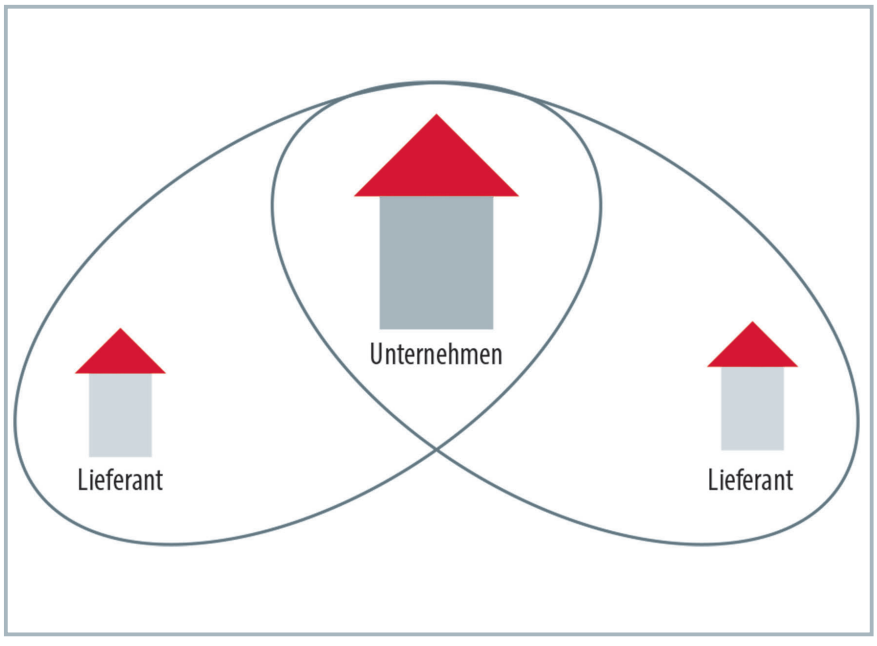

Bild 1. **Einbeziehung Ihrer Lieferanten in den Schutz der Informationswerte** Quelle: DQS GmbH, © Hanser

wie bewährt: Ihre Kunden erwarten von Ihnen Qualität und Sie gleiches von Ihren Lieferanten. Aus dem Blickwinkel der Tisax-Anforderungen erfordert dies analog auch die Einbeziehung Ihrer Lieferanten in den Schutz der Informationswerte. Auch hier lohnt ein eingehender Blick auf die Schutzziele, denn zuweilen erweitert sich damit die Liste der einzubeziehenden Lieferanten.

- Ein Lieferant, welcher Verbrauchsmaterial oder Standardkomponenten zur Verfügung stellt, erhält selten schützenswerte Informationen.
- Gemeinsame Entwicklung erfordert hingegen auch den Austausch von Informationen, sodass auf deren Vertraulichkeit zwingend Wert zu legen sein wird. In der Regel kommen hier NDAs (non-disclosure agreements) zum Einsatz.
- Bedienen Sie sich eines externen Rechenzentrums, so werden mit diesem neben der Vertraulichkeit auch Fragen der Datenintegrität und der Verfügbarkeit zu diskutieren sein. Rahmenverträge regeln in diesen Fällen beispielsweise die Verfügbarkeit der Services oder SLAs (service level agrements, den Leistungsumfang oder die Reaktionsgeschwindigkeit.
- Da der Zugang zum externen Rechenzentrum auf die Dienstleistungen von Telekommunikationsanbietern zurückgreifen muss, wird deren Verfügbarkeit im Vordergrund stehen.
- Einem externen Reinigungsdienstleisten gegenüber erlauben Sie bspw. nur den Zugang zu bestimmten Unternehmensbereichen, fordern die Vernichtung der Papierabfälle in definierter Weise ein oder sprechen nur bestimmten Personen aus diesem Unternehmen Ihr Vertrauen und damit die Zugangsberechtigung aus.

Unsere Empfehlung

Diese Beispiele verdeutlichen, dass Lieferanten bezogen auf deren Leistung von Fall zu Fall durchaus unterschiedlich einbezogen werden müssen. Entsprechend differenziert sollten sich Ihre Maßnahmen darstellen.

Während sich bei dem einen Lieferant nichts ändern könnte, gehen Sie im anderen Fall zu einer Überarbeitung der vertraglichen Rahmenbedingungen unter Berücksichtigung der Informationssicherheit über. Wiederum in einem anderen Fall erachten Sie eine Teilnahme am Tisax-Verfahren als zwingend oder sehen in ihren Lieferantenaudits den Schwerpunkt Informationssicherheit vor.

Neben der Angemessenheit in diesem Vorgehen ist dabei die kontinuierliche Überprüfung der von ihnen getroffenen Einstufungen Ihrer Lieferanten von Bedeutung.

Denn nichts ist so beständig wie die Veränderung der Risiken und der Bedeutung von Informationen. ■

INFORMATION & SERVICE

BEITRAGSREIHE

Die dreiteilige Beitragsserie zu Trusted Information Security Assessment Exchange (Tisax), dem branchenspezifischen Framework für Informationssicherheit in der Automobilindustrie wird fortgesetzt.
Teil 1 Schritt für Schritt zum Assessment. Informationssicherheit in der Automobilindustrie: Der Blick aufs Ganze ist in QZ 7/2021 erschienen.
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