Whitepaper „Harmonisierung der Klassifizierungsstufen“

Schutzziel: Vertraulichkeit

Version: 1.0
Datum: 19.04.2018
Klassifizierung: öffentlich/public

VDA | Verband der Automobilindustrie

Inhalt

Einleitung/Motivation

Informationssicherheit ist für Unternehmen von entscheidender Bedeutung. Durch zunehmende Vernetzung und Informationsaustausch innerhalb der Wertschöpfungskette wird diese zukünftig noch weiter steigen.

Der Arbeitskreis Informationssicherheit des Verbands der Automobilindustrie (VDA[1]) hat die grundsätzlichen Anforderungen bezüglich Informationssicherheit im VDA ISA[2] (Information Security Assessment) Katalog beschrieben, der bei Sicherheitsüberprüfungen angewendet wird. Als Arbeitskreis möchten wir darüber hinaus konkrete Hinweise zur Umsetzung der Anforderungen geben.

Eine wesentliche Grundlage zur Erreichung eines bedarfsgerechten Informationssicherheitsniveaus bilden die Informationsklassifizierung und die Kennzeichnung von Informationen. Sie haben den Zweck, Informationen abhängig vom Wert für ein Unternehmen in verschiedene Klassifizierungsstufen einzuordnen.

Für diese Klassifizierungsstufen werden im VDA ISA Katalog organisatorische und technische Anforderungen festgelegt, die mit einem angemessenen und zweckmäßigen Aufwand zur Erreichung der Sicherheit der entsprechenden Informationen führen sollen.

Die meisten Unternehmen haben bereits Klassifizierungsstufen implementiert, das heißt, ein Schema zur Informationsklassifizierung beschrieben und durch entsprechende Richtlinien etabliert.

Ein Vergleich innerhalb der Automobilindustrie hat gezeigt, dass es sowohl bei der Anzahl als auch bei der Bezeichnung der Klassifizierungsstufen Unterschiede zwischen den Unternehmen gibt. Diese Unterschiede können - gerade beim Informationsaustausch - zu Unklarheiten und daraus resultierenden Unsicherheiten führen.

Der Arbeitskreis Informationssicherheit sieht es daher als zweckmäßig und für Unternehmen wirtschaftlich sinnvoll an, ein einheitliches Schema zur Informationsklassifizierung als Standard festzulegen und zur Umsetzung zu empfehlen.

[1] https://www.vda.de/de

[2] https://www.vda.de/de/services/Publikationen/information-security-assessment.html

Das vorliegende Whitepaper beschreibt den Vorschlag des VDA Arbeitskreises Informationssicherheit zur Festlegung eines solchen Schemas mit Fokus auf dem Schutzziel Vertraulichkeit; dieses beinhaltet, dass Informationen unbefugten Personen, Organisationen oder Prozessen nicht zugänglich gemacht werden. Weitere Schutzziele wie z. B. Verfügbarkeit, Integrität oder Belastbarkeit sind nicht Fokus des vorliegenden Whitepaper.

Informationsklassifizierung

Sowohl die Informationssicherheit-Norm ISO/IEC27001 als auch der VDA ISA Katalog setzen die Informationsklassifizierung als wesentliche Anforderung für eine effektive Informationssicherheit voraus.

„Informationen sind anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung zu klassifizieren.“

„Ein angemessener Satz von Verfahren zur Kennzeichnung von Information ist entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt.“

[ISO/IEC27001:2013]

„Inwieweit werden Informationen hinsichtlich ihres Schutzbedarfs eingestuft und gibt es Regeln für Kennzeichnung […]?“

„Ein einheitliches Schema zur Klassifizierung von Informationen ist vorhanden und wird angewendet.“

„Die Einstufung von Informationen erfolgt nach definierten Kriterien, u. a. Wert, gesetzlicher Anforderungen, Vertraulichkeit, Integrität und Verfügbarkeit.“

[VDA ISA 4.0]

Im Rahmen der Informationsklassifizierung (in Bezug auf die Vertraulichkeit) werden die möglichen Auswirkungen (potenzielle Schäden) für in Unternehmen für den Fall bewertet, dass Informationen ungewollt einem unberechtigten Empfängerkreis offengelegt werden.

Durch unangemessene Informationsklassifizierung und dem daraus resultierenden Umgang mit Informationen können Risiken (z. B. Informationsverlust durch Festlegung einer zu niedrigen Klassifizierungsstufe) entstehen, oder unwirtschaftliche Mehraufwände (z. B. durch die Festlegung einer zu hohen Klassifizierungsstufe) verursacht werden.

Im VDA ISA Katalog sind, abhängig vom potenziellen Schaden, für Unternehmen folgende allgemeine Schutzklassen definiert:

Schutzklasse	Beschreibung
normal	Der potenzielle Schaden ist geringfügig, kurzfristiger Natur und auf ein einzelnes Unternehmen begrenzt.
hoch	Der potenzielle Schaden ist beträchtlich oder mittelfristiger Natur oder nicht auf ein einzelnes Unternehmen begrenzt.
sehr hoch	Der potenzielle Schaden ist für das Unternehmen existenzbedrohend oder langfristiger Natur oder nicht auf ein einzelnes Unternehmen begrenzt.

Tabelle 1: Übersicht der Schutzklassen nach VDA ISA

Für das Schutzziel Vertraulichkeit werden in der Praxis diese Schutzklassen dem jeweiligen, unternehmensspezifischen Schema zur Informationsklassifizierung zugeordnet.

Innerhalb der Automobilindustrie gibt es hierfür bisher kein einheitliches Schema - mit der Konsequenz, dass beim Austausch von Informationen über Unternehmensgrenzen hinweg Klassifizierungsstufen unterschiedlich zugeordnet, bezeichnet und interpretiert werden. Dieser Umstand kann somit zu einer ungewollt unterschiedlichen Handhabung von zu schützenden Informationen führen.

Der Arbeitskreis Informationssicherheit des VDA hat sich am 16.11.2017 auf ein vierstufiges Schema zur Informationsklassifizierung verständigt.

Die folgende Tabelle veranschaulicht die empfohlenen Stufen zur Informationsklassifizierung und deren Zuordnung zu den VDA ISA Schutzklassen:

Schutzklasse nach VDA ISA	**Klassifizierungsstufen (Bezeichnung deutsch)**	**Klassifizierungsstufen (Bezeichnung englisch)**
-	Öffentlich	Public
normal	Intern	Internal
hoch	Vertraulich	Confidential
sehr hoch	Streng vertraulich	Strictly confidential

Tabelle 2: Einheitliches Schema zur Informationsklassifizierung

Die Klassifizierungsstufe „Öffentlich“ ist keiner Schutzklasse nach VDA ISA zugeordnet. Sie wird im Rahmen des Whitepapers dennoch berücksichtigt, da viele Unternehmen diese Klassifizierungsstufe verwenden. Die Einstufung und damit einhergehende Verarbeitung von „öffentlichen“ Informationen obliegt in den meisten Unternehmen den dafür autorisierten Stellen (z. B. Unternehmenskommunikation, Marketing).

Die aus den drei weiteren in Tabelle 2 aufgeführten Klassifizierungsstufen/Schutzklassen abgeleiteten Anforderungen zum sicheren Umgang mit Informationen (z. B. Verschlüsselung) sind im VDA ISA Katalog definiert und beschrieben.

Kennzeichnung von Informationen

Eine ordnungsgemäße Kennzeichnung ist eine Voraussetzung dafür, dass Informationen richtig behandelt werden. Daher sollten Informationen gemäß ihrer Klassifizierungsstufe gekennzeichnet werden.

Neben dem Ersteller müssen sowohl Empfänger als auch Verarbeiter von Informationen die Klassifizierungsstufen und die damit verbundenen Anforderungen zum Umgang mit diesen Informationen kennen, verstehen und anwenden.

Insbesondere bei der Weitergabe von vertraulichen und streng vertraulichen Informationen über Unternehmensgrenzen hinweg (z. B. an Partnerfirmen) ist eine Kennzeichnung zwingend erforderlich. Bei der Kennzeichnung sind die Form[3] der Information und ihre Klassifizierungsstufe zu berücksichtigen.

Neben dem einheitlichen Schema zur Informationsklassifizierung und der entsprechenden Kennzeichnung im Dokument sieht der Arbeitskreis Informationssicherheit gerade bei IT-Anwendungen eine einheitliche Kennzeichnung, z. B. einen farblichen Hinweis beim Öffnen einer digitalen Information (z. B. E-Mail, Präsentationsdatei) als wichtiges Merkmal zur Sensibilisierung an.

Damit wird dem Empfänger visuell die Klassifizierungsstufe einer digitalen Information deutlich gemacht. Darüber hinaus schafft ein farblicher Hinweis (z. B. in Form eines farbigen Balkens) ein einheitliches Verständnis der Klassifizierungsstufe, unabhängig von länder- und sprachspezifischen Unterschieden (siehe Tabelle 3).

[3] z. B. digital, physisch, mündlich

Schutzklasse nach VDA ISA	Klassifizierungsstufen	Farblicher Hinweis (bei IT-Anwendungen)
-	Öffentlich	-
normal	Intern	Grün
hoch	Vertraulich	Gelb
sehr hoch	Streng vertraulich	Rot

Tabelle 3: Zuordnung von Farblichen Hinweis zu Klassifizierungsstufen

Fazit und Empfehlung

Das vorliegende Whitepaper gibt eine Orientierung zu harmonisierten und standardisierten Klassifizierungsstufen in Bezug auf die Vertraulichkeit und trägt in Zusammenhang mit den Anforderungen des VDA ISA dazu bei, Missverständnissen und Risiken beim Informationsaustausch vorzubeugen und damit einen angemessenen Umgang mit Informationen zu ermöglichen.

Der VDA empfiehlt seinen Mitgliedern, sich an diesem Whitepaper zu orientieren und in den Unternehmen das beschriebene Schema zur Informationsklassifizierung umzusetzen.

Autorenverzeichnis

Name	Unternehmen	E-Mail-Adresse
Jens Frölich	AUDI AG	jens.froelich@audi.de
Thomas Donner	BMW AG	thomas.donner@bmwgroup.com
Oliver Schmitt	Robert Bosch GmbH	oliver.schmitt@de.bosch.com
Jürgen Rilling	Daimler AG	juergen.rilling@daimler.com
Thomas Harich	MAHLE GmbH	thomas.harich@mahle.com
Matthias Teuscher	Rheinmetall AG	matthias.teuscher@de.rheinmetall.com
Burkhard Kesting	ZF Friedrichshafen AG	burkhard.kesting@zf.com

Dokumenten- und Versionshistorie

Version	Datum	Status, Anmerkungen
1.0	19.04.2018	Final