Hardwareinventarisierungen enthalten wichtige Informationen für Datenschutzbeauftragte

Zusammenfassung: Datenschutzbeauftragte müssen wissen, mit welchen Geräten eine Verarbeitung personenbezogener oder auf Personen beziehbarer Daten erfolgt. Kaum ein Unternehmen verfügt jedoch über eine aktuelle Inventarliste Hardware die diese Anforderungen erfüllt. Daher können Datenschutzbeauftragte ihre Aufgabe der Überprüfung (Art. 39 Abs. 1b EU-DSGVO) nicht vollständig wahrnehmen. Der folgende Praxistipp enthält wichtige Informationen zu Erfordernis, Einführung und Umsetzung der Hardwareinventarisierung aus Sicht des Datenschutzes.

Der Praxisfall: Router werden außer Betrieb genommen. Mitarbeiter der IT haben einen Dienstleister, der sich vertraglich verpflichtet hat, die Router datenschutzkonform zu entsorgen. Die Router enthalten beim Verlassen des Unternehmens noch Daten, von denen zumindest ein Teil personenbezogen oder auf Personen beziehbar ist. Mindestens einer der Router wird in der Folge im Internet angeboten. Ein versierter Anwender erwirbt den Router prüft ihn auf enthaltene Daten. Diese sind so brisant, dass er zumindest auf die interne Netzwerkebene hätte gelangen können. Von dort aus ist es für einen erfahrenen Administrator relativ leicht weiter in das Netz vorzudringen und irgendwann auch personenbezogene Daten einzusehen. Er stellt anhand von eindeutigen Einträgen fest, welches Unternehmen diesen zuvor verwendet hatte. Er meldet sich dort, aber alle seine Gesprächspartner streiten ab, mit besagtem Router etwas zu tun zu haben. Er wird weder nach Typ noch nach Gerätenummer gefragt, stattdessen barsch abgewiesen – („Das kann überhaupt nicht sein!“) Verärgert wendet er sich an die Öffentlichkeit.

Der Fehler und die Folgen: Mit einer Inventarliste der Netzwerkgeräte hätte leicht festgestellt werden können, dass das Gerät tatsächlich aus besagtem Unternehmen stammt, wie auch immer es ins Internet gelangte. Der Datenschutzvorfall ist perfekt, ein Bußgeld in 6-stelliger Höhe die Folge.

Hardwareinventar: Dabei handelt es sich um eine möglichst vollzählige Aufstellung aller Hardwarekomponenten, die bei der Verarbeitung von Daten, auch personenbezogenen Daten, zum Einsatz kommen. Wichtig für Datenschutzbeauftragte ist hierbei, dass wirklich alle Hardwarekomponenten, also auch Mobiltelefone/Smartphones, Kameras, Navigationsgeräte in Dienstfahrzeugen, Massenspeicher wie USB-Sticks und SD-Karten sowie Ein- und Ausgabegeräte wie Faxgeräte oder Drucker im Hardwareinventar aufgeführt sind.

Was ich nicht weiß, macht mich (nicht?) heiß: Datenschutzbeauftragte, IT-Mitarbeiter und alle anderen in der Organisation können naturgemäß nur über Bekanntes urteilen oder Entscheidungen treffen. Was glauben Sie als Datenschutzbeauftragte, wie viele Geräte mit personenbezogenen Daten es in der Organisation gibt, von denen sie nichts wissen? Vorsicht: Mit der Schulter zucken und sagen, das ist dann halt so, kann gefährlich werden. Wie sollen Datenschutzbeauftragte die in der EU-DSGVO und den nationalen Gesetzen zur Vertiefung genannten Überwachungsaufgaben (Art. 39 Abs. 1b EU-DSGVO) einhalten, wenn Geräte im Einsatz sind, von denen nichts bekannt ist und mit denen personenbezogene Daten oder auf Personen beziehbare Daten verarbeitet werden? Wie sollen die Anwender dieser Geräte mit den Gefährdungen und Risiken vertraut gemacht werden, die beim täglichen Umgang mit diesen nicht erfassten Geräten drohen, insbesondere für personenbezogene Daten? Mich als Datenschutzbeauftragter sollte also gerade das heiß machen, was ich NICHT weiß!

Hardwareinventar ist Chefsache: Da mit unbekannten Geräten Verletzungen der Persönlichkeits- und Freiheitsrechte der Betroffenen geschehen können, ist die Information über alle genutzten Geräte für die Umsetzung des Datenschutzes unabdingbar. Somit ist ein Hardwareinventar erforderlich. Die EU-DSGVO fordert die Umsetzung des Datenschutzes als Managementsystem zu organisieren. Die Inhalte der Art. 24 und Art. 5 Abs. 2 geben an, dass jedes Unternehmen ein Datenschutz-Management-System braucht, um den Schutz personenbezogener Daten leisten zu können. In Art. 5 Abs. 2 heißt es „Der Verantwortliche ist für die Einhaltung des Absatzes 1 (Anmerkung: der Grundsätze für die Verarbeitung personenbezogener Daten) verantwortlich und muss die Einhaltung nachweisen können (Rechenschaftspflicht)“ Die Erfüllung dieser Rechenschaftspflicht kann nach geltendem Verständnis nur mit Hilfe eines Managementsystems erfüllt werden. Jedes Managementsystem, und damit auch ein Datenschutz-Management, setzt die Übernahme der Gesamtverantwortung für sicherheitsrelevante Prozesse durch die Leitung voraus.

Hardware definieren: Eine gängige Definition von Hardware beschränkt sich auf PCs und andere Computersysteme. Dazu gehören dann das Gerät selbst mit Festplatte und

Motherboard, Eingabegeräte wie Tastatur und Maus sowie Ausgabegeräte wie Monitor/Bildschirm und Drucker. Das ist jedoch viel zu kurz gegriffen. Aus Sicht des Datenschutzes muss ein Hardwareinventar alle funktionalen Komponenten erfassen, auf denen personenbezogene oder auf Personen beziehbare Daten enthalten sein können. Das sind – wie schon weiter oben erwähnt – naturgemäß viel mehr Hardwarekomponenten als die reinen Rechner. Die erste Aufgabe für die Erstellung eines aus Sicht des Datenschutzes verwertbaren Hardwareinventars besteht also darin, eine umfassende Liste mit der zu erfassenden Hardware zu erstellen.

Prozessorganisation: Selbst wenn eine Hardwareinventarisierung durchgeführt wird, werden oftmals nicht alle Hardwarekomponenten erfasst. Das kann daran liegen, dass zum Zeitpunkt der Inventarisierung einzelne Mitarbeiter – und mit ihnen die Geräte – nicht anwesend sind. Das kann daran liegen, dass Hardwarekomponenten derzeit nicht verwendet werden und in Schränken oder Abstellräumen „übersehen“ wurden. Damit ein Prozess optimal ausgeführt werden kann, müssen die Abläufe strukturiert erfolgen. Dies gilt nicht nur für die möglichst effiziente Umsetzung des Prozesses sondern auch für die gesetzeskonforme Umsetzung, insbesondere auch hinsichtlich der datenschutzrechtlichen Vorgaben.

Beschreibung der Verarbeitungstätigkeit vornehmen: In der EU-DSGVO wird eine Übersicht über die Verarbeitungstätigkeiten verlangt. Für die einzelnen Verarbeitungstätigkeiten, früher auch Verfahren und Verfahrensbeschreibung genannt, müssen aussagefähige Beschreibungen der Abläufe und der datenschutzrechtlichen Rahmenbedingungen vorliegen. Da bei der Hardwareinventarisierung auch personenbezogene Daten erfasst werden könnten (Das Gerät ist Herrn / Frau X zugeordnet – beispielsweise Mobiltelefone) handelt es sich um eine Verarbeitungstätigkeit im Sinne von Art. 30 EU-DSGVO. Demzufolge ist eine entsprechende Beschreibung anzufertigen.

Prozessanweisung bzw. Arbeitsanweisung: Eine verbindliche schriftliche Vorgabe, wie der Prozess ablaufen soll, ist für wiederkehrende Prozesse auf Dauer unabdingbar. In der Regel glauben die Beschäftigten, die regelmäßig im Prozess Inventarliste Hardware tätig sind, diese verbindlichen schriftlichen Vorgaben nicht zu benötigen. Das ist jedoch ein Trugschluss. Schon bei einer unvorhersehbaren Verhinderung eines dieser Beschäftigten kann zu Störungen im Prozessablauf führen. Je komplexer die Geschäftsprozesse miteinander verwoben sind, desto wichtiger ist deren reibungsloser Ablauf. Daher sind verbindliche schriftliche Vorgaben zu den Prozessabläufen unverzichtbar.

Rechtmäßigkeit der Verarbeitung klären: Aus Sicht des Datenschutzes muss jeder Prozess, bei dem personenbezogene Daten verarbeitet werden, durch eine Rechtsgrundlage legitimiert sein. Wird eine Inventarliste Hardware für definierte Zwecke benötigt, beispielsweise aus Erwägungen der Informationssicherheit, dann handelt es sich um eine Verarbeitungstätigkeit, die in das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO auszunehmen ist. Aus diesem Grund sollte die Rechtsgrundlage, aufgrund derer die Inventarliste Hardware geführt werden darf, geklärt sein. Ist dies nicht der Fall, kann es sich um eine nicht gesetzeskonforme Verarbeitungstätigkeit handeln. Dies könnte in der Folge zu einem Bußgeld führen. Diese Rechtsgrundlage dürfte im vorliegenden Fall auf Art. 6 Abs. 1f EU-DSGVO basieren (Rechtmäßigkeit der Verarbeitung –berechtigte Interessen der Verantwortlichen).

Achtung Auftragsverarbeiter: Im Rahmen einer Auftragsdatenverarbeitung können Auftraggeber im Vertrag fordern, dass Auftragnehmer offenlegen, mit welchen Geräten der Auftrag erfüllt wird. Bei der Erfüllung dieser vertraglichen Auflage wird eine komplette oder partielle Inventarliste Hardware erstellt. Alternativ kann aus einer bestehenden Inventarliste Hardware ein Auszug erstellt und für den geforderten Zweck zur Verfügung gestellt werden.

Mit eigenen Ressourcen oder mit Unterstützung: Beim Prozess Inventarliste Hardware kann es sich um einen Prozess handeln, der ausschließlich mit eigenen Ressourcen abgearbeitet wird, es kann jedoch auch sein, dass externe Unterstützung hinzugezogen wird. Wenn innerhalb einer Unternehmensgruppe ein Schwesterunternehmen, Tochterunternehmen oder die Zentrale den Prozess unterstützt, handelt es sich datenschutzrechtliche ebenfalls um externe Unterstützung. Wird externe Unterstützung hinzugezogen, sind mit diesen (den Dienstleistern) Verträge so abzuschließen, dass diese den Anforderungen an den Datenschutz gemäß Art. 28 EU-DSGVO entsprechen. In diesem Fall müssen wir als Verantwortlicher mit den Auftragsverarbeitern spezielle Vereinbarungen treffen, damit die Anforderungen der EU-DSGVO erfüllt werden.

ADV nach EU-DSGVO bedeutet in Kurzform: Sorgfältige Auswahl der Dienstleister nach hier vorgegebenen Kriterien vornehmen, spezielle Vertragsklauseln mit hier vorgegebenen Mindestinhalten anwenden, Berücksichtigung der besonderen Aufgaben und Pflichten des Auftragsverarbeiters bei der geplanten Verarbeitung, ermitteln der Risiken für die Rechte

und Freiheiten der betroffenen Person, Kontrollen durchführen oder Zertifizierungen dokumentieren als Beleg für die Umsetzung der Regeln, Umgang mit den Daten nach Ende der Zusammenarbeit regeln.

Hardwareinventar aktuell halten und Reaktionen auf Unstimmigkeiten: Ist ein Hardwareinventar erstellt, muss es auch aktuell gehalten werden. Außerdem müssen Unstimmigkeiten überprüft werden. Bei vermissten oder verschwundenen Geräten muss außerdem klar sein, ob Daten enthalten sind, die eine Data Breach Notification auslösen. Zu diesen Fragen folgt ein eigener Praxistipp.

Ein kleiner Ausblich in die schöne neue Welt von morgen: Vielleicht gibt es eines Tages eine Drohne als persönlichen Assistenten des Datenschutzbeauftragten. Also quasi eine Kollegin aller zu erfassenden Hardwarekomponenten. Diese könnte dann die Aufgabe erhalten, loszufliegen und alle noch nicht erfassten „Kollegen“ aufzuspüren. Stellt sich erstens die Frage, ob sich Datenschützer solche Heinzelmännchen wirklich wünschen – und zum anderen schleicht sich da schon der heimliche Verdacht ein, dass es dann Hardwarekomponenten geben könnte, die so programmiert sind, dass sie die Datenschutzdrohne davon überzeugen, vielleicht mit einer Einladung zum sanften Ölen, dass sie nicht anwesend sind. Schöne neue Welt?!

Eberhard Häcker, Ensdorf

Der Autor Eberhard Häcker ist Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und seit vielen Jahren als Externer Datenschutzbeauftragter und Datenschutzberater tätig. Seine Fachaufsätze erscheinen regelmäßig in unterschiedlichen Publikationen. Außerdem ist er Geschäftsführer der HäckerSoft GmbH, die unter anderem mit der Datenschutzsoftware DATSIS und der Lernplattform Optilearn (Pflichtschulungen für Datenschutzbeauftragte) am Markt aktiv ist. Sein Lieblingsprojekt ist datenschutzkabarett.de.