Praxistipps Datenschutz 08 2017

Ortsbegehungen – Soft- und Hardware mit personenbezogenen Daten

Zusammenfassung: Ortsbegehungen sind für Datenschutzbeauftragte unverzichtbar. Im vorliegenden Praxistipp geht es vor allem um die Aufnahme der vorhandenen Geräte und die Software, die mit diesen Geräten genutzt wird.

Der Praxisfall: Ortsbegehung bei Datenschutz und IT-Sicherheit. Im Unternehmen sind Inventarnummern Standard. Allerdings finden sich in etlichen Räumen noch Geräte, mit denen früher einmal gearbeitet wurde und auf denen mutmaßlich noch personenbezogene Daten schlummern, die aber von der Inventarisierung nicht erfasst sind. Für Datenschutzbeauftragte Alltag, aber noch lange nicht schön. Zeit, sich um diese verwaisten Geräte zu kümmern. Dafür sind Ortsbegehungen ideal.

Inventarisierung oder nicht? Liegt im Unternehmen eine Inventarisierung vor, sollte in Absprache mit der inventarisierenden Stelle (in der Regel die IT) bei allen aufgefundenen Geräten geprüft werden, ob die Inventarisierungsnummer vorhanden ist oder nicht.

Publikumsverkehr oder nicht? In Räumen, in die ständig andere als dort arbeitende Personen kommen (Publikumsverkehr), ist zu prüfen, ob die Arbeitsplätze vor unbefugter Dateneinsicht hinreichend geschützt sind. Befinden sich Drucker, Faxgeräte oder allgemein Multifunktionsgeräte im Raum, ist in diesem Fall die Faxausgabe so vorzunehmen, dass Ausdrucke oder Faxe mit dem Schriftbild nach unten ausgegeben werden.

Multifunktionsgeräte: Wenn im Büro Multifunktionsgeräte stehen, heißt das in aller Regel auch durch deren Nutzung bedingt vermehrter Publikumsverkehr. Nicht nur das Gerät selbst muss dann unter besonderer Aufsicht stehen, auch die personenbezogenen Daten an den einzelnen Arbeitsplätzen sind besonders sorgfältig vor unbefugter Einsichtnahme zu schützen. Dies gilt besonders bei Arbeitsplätzen die in der Nähe des Multifunktionsgerätes stehen oder von dort aus eingesehen werden können. Die Speicher der Multifunktionsgeräte sind regelmäßig zu löschen. Wartung darf nur im Beisein von geeigneten Beschäftigten vorgenommen werden, außerdem ist zu prüfen, ob die Geräte Festplatten haben, ob diese verschlüsselt sind und was mit diesen bei Rückgabe des Leasinggerätes oder bei Verkauf geschieht.

Drucker: Die Zahl der Arbeitsplatzdrucker oder gemeinschaftlich genutzten Drucker ist aufzunehmen. Es ist zu klären, ob es sich um Netzwerkdrucker handelt oder um Einzelplatzlösungen. Es ist zu klären, ob die Wartung intern oder extern erfolgt. Entsprechend ist zu prüfen, ob ein Vertrag über Datenverarbeitung im Auftrag erforderlich ist oder nicht, beziehungsweise ob ein solcher schon vorliegt, falls dieser erforderlich sein sollte.

Server: In immer weniger werdenden Fällen können sich auch Server (Hardware) im Raum befinden. Hier ist zu prüfen, inwieweit diese dann vor unbefugtem Zugriff geschützt sind. Befindet sich der Arbeitsplatz der für den Server verantwortlichen Person im Raum, ist das auch festzuhalten und anders zu bewerten, als wenn das nicht der Fall sein sollte. In jedem Fall sollten Server ausschließlich in dafür besonders geeigneten Räumen stehen. Sind die Server im Raum, weil auch die dahinter stehende Funktionalität im Raum benötigt wird (beispielsweise der Personalserver im Personalbüro), ist auch die zum Einsatz kommende Software von Interesse. Bitte auch nach möglichen Servern in Nebenräumen fragen, die nur über den begutachteten Raum betreten werden können.

PCs und Thin Clients: Diese Geräte sind fest verbaut und für den Einsatz nur in dem betreffenden Büro vorgesehen. Sie sind in der Regel so eingerichtet, dass sich jeder mit seinem Usernamen und dem persönlichen Passwort anmelden kann. Neben der Anzahl der im Raum befindlichen Geräte ist auch von Interesse, ob die übliche Bürosoftware verwendet wird oder ob spezielle Software auf den Geräten enthalten ist, die möglicherweise auch im Softwareinventar gar nicht vorhanden ist. Solche Geräte können auch nur vorgehalten werden, werden aber aktuell nicht genutzt. In diesem Fall ist zu prüfen, ob und in welchem Umfang personenbezogene Daten auf den Geräten enthalten sind.

Notebooks: Notebooks sind zumeist für den persönlichen Einsatz vorgesehen. Es können aber auch Geräte im Raum sein, die keine personenbezogenen Daten beinhalten, sondern ausschließlich für Zwecke der Präsentation vorgesehen sind. In diesem Fall sollte auch gefragt werden, ob bekannt ist, wie dann Sicherheitsupdates oder das Update von Virenscannern erfolgen. Wenn Notebooks mit einer Dockingstation versehen sind, so ist de-

ren Einsatz im Unternehmen an einem festen Arbeitsplatz vorgesehen. Grundsätzlich sollte gefragt werden, ob die Festplatten der Notebooks verschlüsselt sind. Bitte auch nach Notebooks in Schränken oder Containern fragen.

Tablets: Glaubt man den Trendforschern, dann haben die Tablets bald die PCs und Notebooks abgehängt. Tablets können mit Tastaturen und zusätzlichen Bildschirmen versehen sein. Zu klären ist, ob sie per LAN-Kabel oder über das WLAN mit den Unternehmensnetzen verbunden sind. Zu klären ist außerdem, ob die private Nutzung untersagt, geduldet oder ausdrücklich erlaubt ist. Befinden sich Tablets im Raum, könnten es sich dabei grundsätzlich auch private Geräte handeln. Auch das sollte geklärt werden.

Mobiltelefone dienstlich: Dienstliche Mobiltelefone sind ebenfalls zu erfassen. Hier ist zu klären, ob diese auch für private Zwecke benutzt werden dürfen und auch benutzt werden. Es ist außerdem zu klären, ob das Smartphone in einem betrieblichen Mobile Device Management eingebettet ist oder nicht. Die Frage nach genutzten Apps ergänzt die Übersicht. Bei den Apps kann es sich um Apps handeln, die auf einer Whitelist (Liste der erlaubten Apps) enthalten sind. Ob bei der Ortsbegehung eine vollständige Liste der genutzten Apps zu erhalten ist, ist eher fraglich. Im Zweifelsfall kann hier die IT Auskunft erteilen. Wenn nicht, handelt es sich um ein ungeklärtes Risiko für Datenschutz und IT-Sicherheit im Unternehmen.

Mobiltelefone privat: Bei privat genutzten Mobiltelefonen ist zu klären, ob deren Nutzung am Arbeitsplatz erlaubt, geduldet oder untersagt ist. Da private Mobiltelefone je nach aufgespielten Apps umfangreiche Datentransfers an die Hersteller der Apps vornehmen, ist zu klären, ob Mails aus dem betrieblichen Mailsystem auf die Smartphones übertragen werden können und auch tatsächlich übertragen werden. Ist dies der Fall, ist zu prüfen, ob im Unternehmen Vertraulichkeitsvereinbarungen einzuhalten sind, bei deren Zuwiderhandeln Konventionalstrafen fällig werden können. Private Mobiltelefone können außerdem mit einer Spionagesoftware versehen sein, die es Angreifern ermöglicht, sich zu jeder beliebigen Zeit aufzuschalten und mitzuhören. Dies geschieht in aller Regel nicht mit Wissen des Beschäftigten, was jedoch für das Ergebnis nicht von Bedeutung ist. Insofern sollte auch eine Klärung herbeigeführt werden, in welchen Bereichen private Smartphones gänzlich untersagt werden sollen.

Kabeltelefone: Auch hier ist die Zahl von Interesse. Außerdem sollte geklärt werden, ob die Geräte über eine Anrufbeantworterfunktion verfügen. Wenn ja, ist zu prüfen, ob für das Abhören der Nachrichten auf dem Anrufbeantworter eine PIN oder ein Passwort erforderlich ist. Sollte das nicht der Fall sein, besteht die Gefahr, dass jede anwesende Person bei Abwesenheit des Anschlussinhabers die Nachrichten auf dem Anrufbeantworter abhören kann. Dies kann ein Verstoß gegen das Fernmeldegeheimnis sein.

Schnurlose Telefone: Das bei den Kabeltelefonen Gesagte gilt grundsätzlich auch für Schnurlostelefone. Da diese auch aus Versehen liegenbleiben können, ist das Risiko, dass ein nicht gesicherter Anrufbeantworter auf dem Gerät unbefugt abgehört wird, noch größer. Da sie in der Regel nur im Netzbereich des Firmennetzes funktionieren, werden sie in der Regel im Falle eines Diebstahls außerhalb des Geländes wertlos. Andererseits kann man Schnurlostelefone leicht mitnehmen und bei sensiblen Gesprächen auch das Büro verlassen, so dass die Kollegen dort nicht mehr mithören können. So lässt sich auch Diskretion besser wahren.

Telefonanlagen: In seltenen Fällen befinden sich auch Telefonanlagen oder wesentliche Elemente von Telefonanlagen in den zu prüfenden Räumen. In diesem Fall sollte eine Sonderprüfung der gesamten Telefonanlage vorgenommen werden. Solche Räume sollten aber grundsätzlich besonders gut geschützt werden.

Kabelschränke, Switche: Irgendwo müssen Kabelschränke und Switche untergebracht werden. Vor allem in älteren Gebäuden kann das auch Büros treffen. Zwar sind Switche normalerweise in verschlossenen Schränken oder in Nebenräumen untergebracht, aber es kann zahlreiche Gründe geben, warum diese gerade einmal nicht verschlossen sind. In diesem Fall ist zu klären, warum das so ist. Hier sollten individuelle Abhilfemaßnahmen vorgesehen werden.

Andere Geräte: Manchmal finden sich auch andere Geräte, mit denen personenbezogene Daten erhoben, verarbeitet und genutzt werden können, in den zu begutachtenden Räumen. Dabei kann es sich um Barcodeleser handeln, um Handscanner oder um andere Geräte in dieser Art. Hier ist zu klären, welchem Zweck diese dienen, ob die dahinter stehenden Verfahren schon Bestandteil des Verfahrensverzeichnisses sind und ob dieser Geräte fremdgewartet werden. Ist dies der Fall, sollte geprüft werden, ob ein Vertrag über Auf-

tragsdatenverarbeitung erforderlich ist oder nicht.

Speichersticks: Nicht selten liegen bei der Ortsbegehung auch Speichersticks auf den Schreibtischen. Dabei kann es sich um private Sticks handeln, aber auch um unternehmenseigene. Bei der Gelegenheit kann auch gleich geprüft werden, ob die USB-Ports für Massenspeicher gesperrt sind oder nicht.

Andere Speicher wie CDs und SD-Cards: Hier ist zu prüfen, ob Geräte vorhanden sind, die derartige Laufwerke haben, und ob entsprechende Speichersticks oder –karten genutzt werden bzw. vorhanden sind. Auch hier sollte geprüft werden, ob die Laufwerke so konfiguriert werden können, dass nur zugelassene Speichereinheiten genutzt werden können.

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