DSGVO – 11/2020

DSGVO – 11/2020

[expand title="mehr lesen…"]

Wo versteckte personenbezogene Daten lauern

Böse Überraschung

Martin Gerhard Loschwitz

Durch die Löschpflicht der DSGVO können vergessene Datensenken im Unternehmen zu einem echten Problem und verdammt teuer werden. Wo liegen heikle Daten, wie stöbert man sie auf und wie verhält es sich mit WORM-Archiven? iX hilft bei der Spurensuche.

-tract

- Die DSGVO sieht Löschpflichten für personenbezogene Daten vor, die nicht länger benötigt werden.
- Für Administratoren gerät der Versuch, die DSGVO-Vorschriften unter anderem mit Archivierungspflichten in Einklang zu bringen, oft zu einer Gratwanderung.
- Vielen Unternehmen ist gar nicht klar, wo sie überhaupt personenbezogene Daten speichern.
- Wichtig ist es, IT-Verantwortliche für versteckte Datensenken mit personenbezogenen Daten zu sensibilisieren, denn die technischen Lösungen für das Problem sind komplex und in vielen Fällen

unbefriedigend.

Man stelle sich im eigenen Unternehmen die folgende Situation vor: Der Drucker druckt nicht. Alles Wackeln am Kabel vermag das Problem nicht zu beseitigen, und letztlich stellt sich heraus, dass der Kollege Niemeyer sich auf seinem Rechner einen Virus eingefangen hat, der das gesamte System lahmlegt. Weil Herr Niemeyer sich den Virus eingefangen hat, indem er auf dubiosen Seiten unterwegs war, und weil seine Personalakte weitere unschöne Einträge enthält, setzt das Unternehmen ihn vor die Tür.

Ein halbes Jahr später – der Prozess vor dem Arbeitsgericht gegen Herrn Niemeyer ist noch in vollem Gange – flattert ein Brief der Landesdatenschutzbehörde ins Haus. Der Rechtsabteilung zieht es prompt die Schuhe aus: 500000 Euro, so heißt es dort, werden in Form einer Strafe wegen Verstoßes gegen die DSGVO fällig. Die Behörde habe stichhaltige Beweise dafür, dass das Unternehmen es seit Jahren versäume, Daten mit persönlichem Bezug im Sinne der DSGVO zu löschen, wenn diese nicht länger benötigt würden.

Klingt wie das Drehbuch eines schlechten Films, ist leider aber überhaupt nicht unwahrscheinlich. Die Datenschutzbehörden der Länder gehen mittlerweile alles andere als zimperlich mit Verstößen im DSGVO-Kontext um, wie das Beispiel Deutsche Wohnen eindrücklich bestätigt. Maja Smoltczyck, die Landesdatenschutzbeauftragte von Berlin, will von der Wohnungsgesellschaft 14,5 Millionen Euro Bußgeld eintreiben, und das mit eben diesem Vorwurf. Zwar wehrt sich die Deutsche Wohnen mit Händen und Füßen und wohl bald auch vor Gericht gegen den Bußgeldbescheid. Und in diesem Fall liegen die Dinge auch etwas anders, weil es hier nicht ein ehemaliger Mitarbeiter war, der den Stein ins Rollen brachte, sondern eine Kooperation mehrerer Datenschutzgruppen.

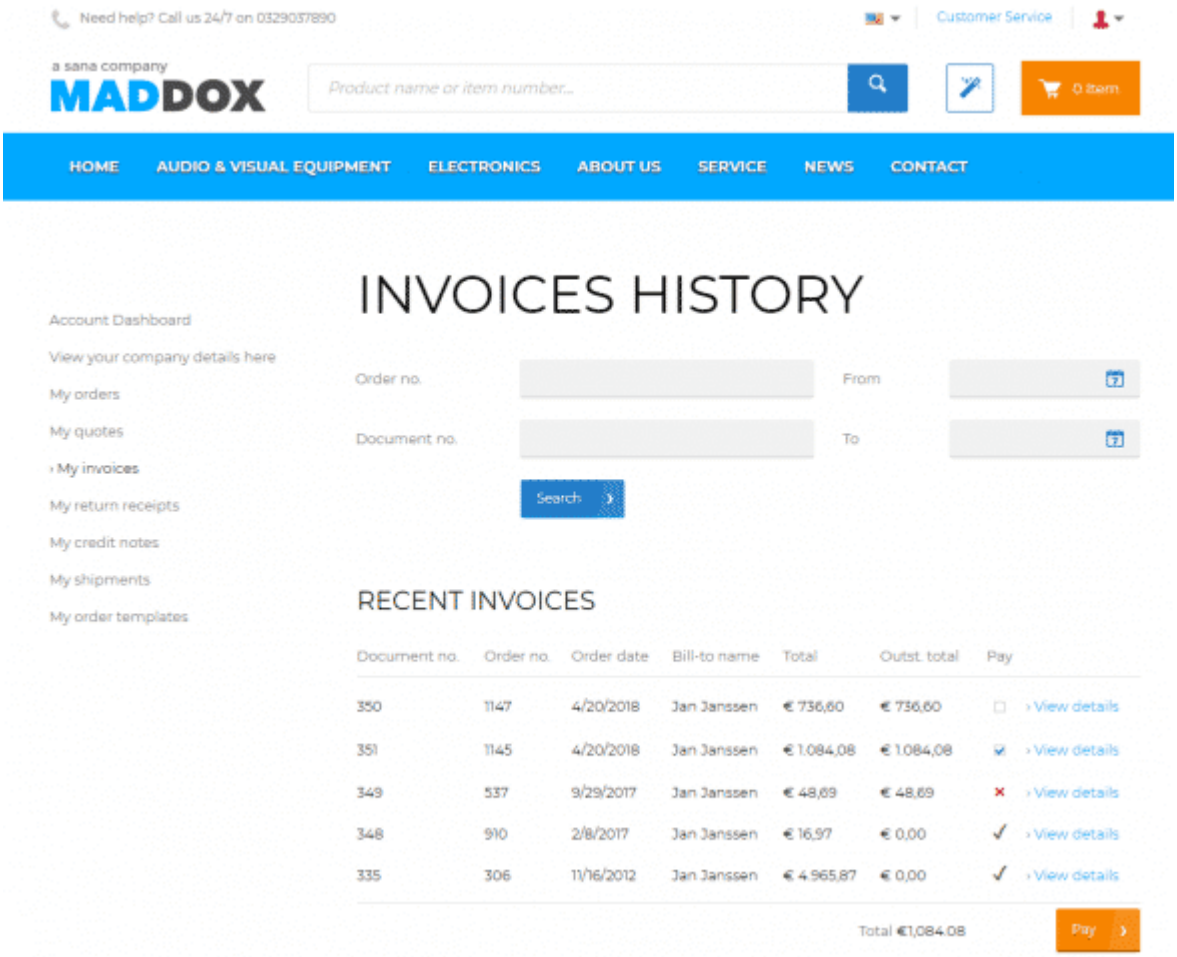
Das Beispiel zeigt jedoch eindrücklich: Die in der DSGVO festgeschriebene Löschpflicht kann für Unternehmen im Fiasko

enden, ohne dass diese auch nur den leisesten Verdacht hätten, was da auf sie zurollt. Und Mitarbeiter mit Rachegelüsten, die über unzulässige Datensenken im Sinne der DSGVO im Unternehmen Bescheid wissen, können erheblichen Schaden anrichten.

Welche Optionen sich Firmen bieten

Was aber können Unternehmen tun? Eines sei gleich am Anfang dieses Artikels gesagt – das Ziel besteht an dieser Stelle nicht darin, über die Löschpflicht im Sinne der DSGVO zu debattieren oder im Detail auf sie einzugehen. Wer sich für die juristischen Spitzfindigkeiten interessiert, möge sich die anderen Artikel der Titelstrecke in dieser Ausgabe zu Gemüte führen. Hier geht es vielmehr um die Praxis – um die IT-Abteilung, die sich als Dienstleister für digitale Services im Unternehmen versteht und mit der DSGVO irgendwie umgehen muss. In dieser Position haben Systemverwalter das ausgesprochen unangenehme Problem, zwischen mehreren Stühlen zu sitzen. Denn bei ihrer alltäglichen Arbeit sind sie ja nicht nur den Regeln der DSGVO unterworfen, sondern auch anderer relevanter Gesetzgebung. Das Finanzamt etwa schreibt vor, dass bestimmte Arten von Belegen revisionssicher über Jahre und Jahrzehnte hinweg für spätere Überprüfungen aufzubewahren sind. Damit besteht im Sinne der DSGVO eine „andere Rechtsgrundlage“ für das Speichern von Daten.

Der Teufel steckt allerdings im Detail: Viele Softwarepakete etwa bieten erst gar keine Möglichkeit, nur bestimmte Teile eines Datensatzes zu löschen, andere jedoch zu erhalten. Verlangt ein Kunde etwa die Löschung seines Benutzerzugangs in einem Webshop, muss das Unternehmen dem Ansinnen grundsätzlich nachkommen, darf aber natürlich die Unterlagen behalten, die aufzubewahren es verpflichtet ist. Die meisten Webshops bieten dafür aber keine Funktion: Wer den Zugang löscht, löscht meist auch sämtliche damit verbundenen Dokumente.



Die DSGVO stellt Unternehmen vor allem bei komplexen Anwendungen wie Shopsystemen vor das Problem, Archivierungs- und Löschpflichten unter einen Hut zu bekommen (Abb. 1). *SANA Commerce*

Ähnliches gilt für Daten, die das Unternehmen nach dem WORM-Prinzip (Write Once, Read Many) zu archivieren verpflichtet ist. Hier kommen oft Hardware-Appliances zum Zug, die den gesetzlichen Vorgaben genügen. Vielfach haben sich Firmen bisher mit dem Thema DSGVO aber nicht ausführlich genug beschäftigt und archivieren ihre Daten erst gar nicht ausreichend fein abgestuft, um der DSGVO zu genügen.

Primär soll dieser Artikel Administratoren sensibilisieren und ihnen Anhaltspunkte dafür liefern, wo sich auf klassischen Serversystemen bedenkliche Daten befinden können. Der Text geht auch auf die Frage ein, welchen Aufwand im Sinne des DSGVO-konformen Speicherns von Daten sie betreiben sollen und müssen und wie sich das mit Tools angenehmer gestalten lässt. Vorrangig jedoch geht es darum, wie Administratoren ihre Sinne

schärfen, um potenziell gefährliche Datensenken im Unternehmen zu erkennen und zu eliminieren.

Datensenken

Der Begriff Datensenke stammt ursprünglich aus den Definitionen im Umfeld von Datenübertragungseinrichtungen (siehe ix.de/z9h2). Dort bezeichnet er eine empfangende Datenendeinrichtung.

In der IT gilt ein weiter gefasster Begriff: Einerseits zählt man nicht nur „empfangende“ Dienste wie Mailserver dazu, sondern generell alle Geräte und Dienste, die Daten vorhalten oder ablegen, vom Benutzerverzeichnis über Datenbanken, Geschäftsanwendungen, Shopsysteme bis hin zu smarten Endgeräten, Syslog-Diensten und Systemeinstellungen. In der Praxis bezeichnet man vor allem solche Orte als Datensenken, wo Daten hingesendet werden, um dort zu versacken – also genau das, was im DSGVO-Kontext zu vermeiden ist.

Viele Unternehmen haben zu wenig getan

Viele Unternehmen müssen sich den Vorwurf gefallen lassen, sich mit dem Thema der in der DSGVO verankerten Löschpflicht erst viel zu spät zu beschäftigen. Als die DSGVO in Kraft trat, gab es die heute aus Sicht von Administratoren unangenehmen Paragrafen ja bereits. Ganze vier Jahre hatten Firmen Zeit, sich technisch auf das vorzubereiten, was eine rigoros angewandte DSGVO für sie bedeuten würde. Passiert ist in dieser Richtung vielerorts wenig.

So ist vielen Verantwortlichen heute leider noch immer völlig unklar, wo in ihren Set-ups personenbezogene Daten anfallen. Viele Admins denken bei personenbezogenen Daten im Sinne der DSGVO zudem automatisch an die Daten der Endanwender. Das ist aber eine unvollständige Sicht auf die Dinge: Der bereits erwähnte Herr Niemeyer hat, wenn im Unternehmen gängige Compliance-Regeln zur Anwendung gekommen sind, einen eigenen

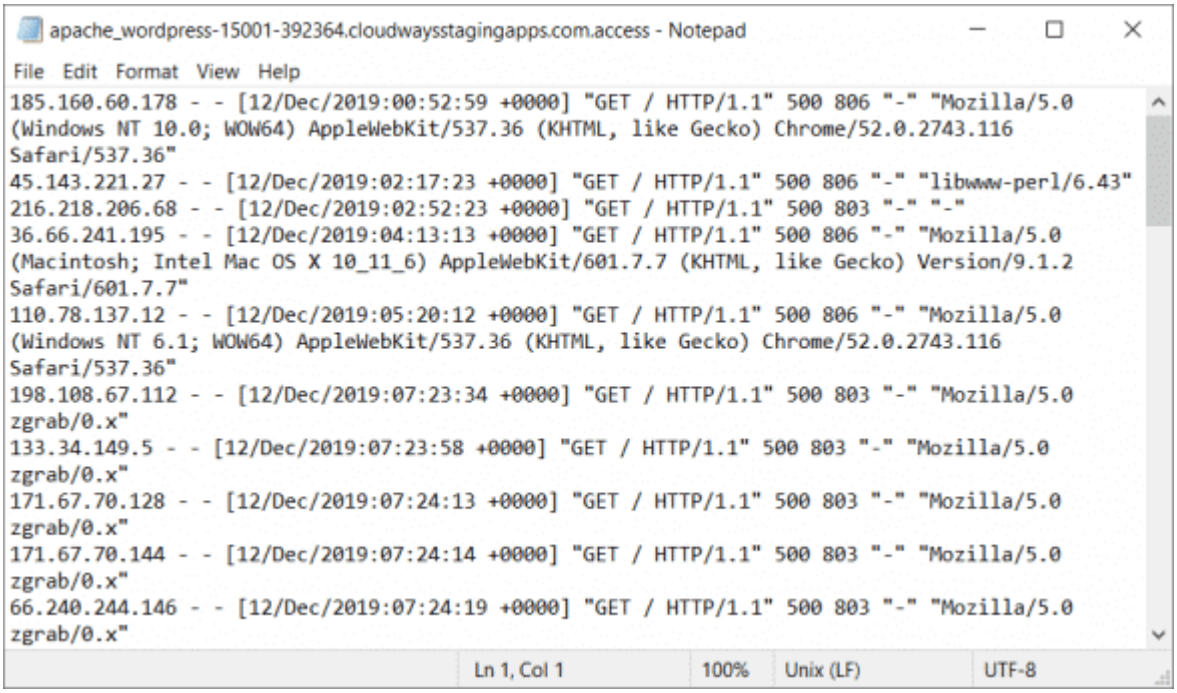
Account gehabt, mit dem er auf den Systemen hantierte.

Personenbezogene Daten sind daher beispielsweise auch die History der Shell, die der nun ehemalige Kollege im Rahmen seiner dienstlichen Tätigkeit genutzt hat. Verlangt er nach einer Einigung vor dem Arbeitsgericht, dass diese Daten entfernt werden, muss die Firma das ebenso tun, wie sie zum Löschen von Kundendaten verpflichtet wäre – freilich unter der einen zentralen Einschränkung, dass jene Daten behalten werden dürfen, zu deren Sicherung die Firma aus anderen Gründen verpflichtet ist.

Dreierlei Werkzeuge im Fokus

Wer vor der Aufgabe steht, Datensenken im eigenen Unternehmen zu finden und zu beseitigen, sieht sich eingangs einer Sisyphusarbeit gegenüber. Denn wenn Hunderte Systeme seit Jahren in Betrieb sind, ist die Wahrscheinlichkeit, dass sich auf diesen personenbezogene Daten finden, ausgesprochen hoch. Grob formuliert gibt es drei Arten von Werkzeugen, mit denen der Admin in diesem Kontext in Berührung kommt.

Da gibt es einerseits die Werkzeuge, die personenbezogene Daten produzieren (etwa die bereits erwähnte Shell in Form ihrer History) oder aufzeichnen (hierzu gehören auch Logdateien aller Art). Dann gibt es die Werkzeuge, deren Aufgabe ja gerade darin besteht, Daten langfristig zu archivieren. Ein solches Werkzeug ist der Firma Deutsche Wohnen zum Verhängnis geworden. Denn die hat Daten wie Gehaltsnachweise, SCHUFA-Auskünfte und ähnliche Unterlagen in ihrem zentralen Archivierungssystem gehabt, lange nachdem die dazugehörenden Mietverträge ausgelaufen waren – ein klarer Verstoß gegen die Löschpflicht, wie Berlins oberste Datenschützerin feststellte.



Ausufernde Webserver-Logs sind keine gute Idee, da auch IP-Adressen zu den personenbezogenen Daten gehören und daher einer Löschpflicht unterliegen (Abb. 2). *Cloudways*

Einfach verzichten können Unternehmen auf diese Geräte aber nicht, denn zum Speichern bestimmter Unterlagen über lange Zeiträume – und zwar revisionssicher – sind sie verpflichtet. Einfache Storage-Systeme reichen hier nicht aus, weil bei bestimmten Datenarten eine nachvollziehbare, nachträglich nicht mehr veränderbare Versionsgeschichte abrufbar sein muss. Dazu kommt spezielle Soft- wie Hardware zum Einsatz, die auf das fein granulierte Speichern von Daten aber nicht ausgelegt ist.

Die dritte Art von Werkzeug sind die Tools, die bei der Suche nach eventuell rechtswidrigen Datensenken unterstützen oder deren Entstehen von vornherein verhindern. Dabei handelt es sich einerseits um klassische Forensikwerkzeuge, mit denen sich versteckte Daten auffinden lassen – andererseits fallen in diese Kategorie aber auch ganz typische Werkzeuge im Kontext der Systemautomation. Die lassen sich möglicherweise auf bestehende Set-ups nur noch schwerlich anwenden, führen vor dem Hintergrund moderner Grundlagen der typischen Systemadministration jedoch dazu, dass Admins das Problem zukünftig umgehen.

Produzenten personenbezogener Daten erkennen

Die erste und oberste Frage bei der Untersuchung einer Umgebung im Hinblick auf personenbezogene Daten ist stets die nach den Datenproduzenten. Welche Programme legen – vor allem unbemerkt – personenbezogene Daten an und speichern sie an Orten, an denen man nicht damit rechnet? Im IT-Kontext der Gegenwart ergeben sich hier leider nahezu beliebig viele Möglichkeiten für Orte, an denen solche Daten anfallen.

Schon ein normales Linux-System bietet eine Vielzahl an Einfallstoren. Stellt man sich etwa einen Host mit Webserver vor, bestehen für die Administratoren vermutlich lokale Benutzeraccounts, über die die Administration erfolgt. Diese beinhalten aller Wahrscheinlichkeit nach zum größten Teil personenbezogene Daten. Teil des Offboardings von Kollegen muss es deshalb sein, auf sämtlichen Systemen etwaige Dateien zu löschen oder rechtskonform zu archivieren, auf die diese Kolleginnen und Kollegen Zugriff hatten. Doch ist es damit noch lange nicht getan, denn personenbezogene Daten fallen auch an anderen Stellen an.

Wer etwa HA-Proxy oder nginx als Load Balancer nutzt, lässt diese vermutlich Logdateien über die Zugriffe anlegen. Ähnliches gilt für Webserver, in deren Logdateien ebenfalls IP-Adressen landen. Der Europäische Gerichtshof hat IP-Adressen – und zwar sowohl dynamische als auch statische – mittlerweile als personenbezogene Daten eingestuft. Damit genießen sie eine besondere Schutzwürdigkeit. Was im Umkehrschluss auch bedeutet: Betreiber von Onlineangeboten dürfen diese Information grundsätzlich nur speichern, wenn damit ein „berechtigtes Interesse“ einhergeht. Die Sicherstellung der Servicequalität sowie die Möglichkeit, im Fehlerfalle Debugging zu betreiben, dürfen wohl als berechtigt wahrgenommen werden.

Wer auf seinen Webservern jedoch Logdateien der vergangenen sechs Monate hat, wird sich mit dem berechtigten Interesse schon schwerer tun: Warum etwa sollte es für den Betrieb eines Webshops von Relevanz sein, ob Ottilie Normalverbraucherin vor drei Monaten eine Bestellung aufgegeben hat, die zwischenzeitlich längst geliefert wurde und somit erledigt ist? Wer nicht schon aus Platzgründen Logrotation betreibt, tut auch im Sinne der DSGVO gut daran, diese zu aktivieren. Analoge Empfehlungen gelten auch für andere Geräte im Netzwerk, etwa Firewalls oder Systeme, die zur Intrusion Detection zum Einsatz kommen.

Datenbanken und Backups: Schatzkiste für Datenschützer

Nahezu jedes zeitgenössische IT-Set-up wird irgendwo eine Datenbank enthalten. Das ist völlig legitim, wenn die gespeicherten Daten nötig sind, um die Geschäftsbeziehung und die beiderseitigen Pflichten zu erfüllen. Das eingangs schon erwähnte Problem der Belege ist mittlerweile vielerorts dringend. Hier treffen zwei Rechtsmaterien aufeinander: die Pflicht der Shopbetreiber, Unterlagen für das Finanzamt aufzubewahren, und die Pflicht, benutzerbezogene Daten zu löschen, wenn sie diese nicht länger benötigen.

Aber: Auf die Datenbank selbst haben Systemverwalter in aller Regel keinen direkten Zugriff. Dieser geschieht oft durch eine Software hindurch, etwa eine Shopsoftware, die die Datenbank im Hintergrund nach eigenem Gutdünken verwaltet. Zwar könnte der Admin händisch an der Datenbank herumpulen – garantieren, dass der Shop danach noch funktioniert, wird dann aber keiner. Die Shopsoftware hingegen bietet die Funktion „Account löschen, aber Belege behalten“ oft einfach nicht. Zwar darf der Admin sich an dieser Stelle mit Fug und Recht aufregen, schließlich hatten die Shopbetreiber seit 2013 Zeit, entsprechende Funktionen einzubauen. Das nicht getan zu haben, grenzt hart an Vorsatz. Doch hat der Admin davon nichts, wenn

ihm die Datenschützer an den Fersen kleben.

Eine befriedigende Lösung gibt es an dieser Stelle leider nicht. Es empfiehlt sich, mit dem Betreiber von Software in Kontakt zu treten und sich über deren abgelegte Daten im Detail zu informieren. Die DSGVO sieht in engen Grenzen Ausnahmen für die Fälle vor, in denen das Löschen dem Anbieter nicht zumutbar ist – dazu später mehr. Möglicherweise lässt sich an der jeweiligen Stelle eine solche Ausnahme zur Anwendung bringen.

Vorsicht ist auch bei Backups geboten. Datenbanken und jede Art von Nutzdaten landen heute zuverlässig in Backups. Systeme mit niedrigem Automatisierungslevel legen zudem oft Logs und andere Nutzdaten in Backups ab. Für diese gilt dasselbe wie für die Daten auf den ursprünglichen Systemen auch: Wer etwa seine Datenbank zwar regelmäßig um nicht länger benötigte Daten erleichtert, diese aber weiterhin im Backup hat, gewinnt in Sachen Datenschutz gar nichts. Theoretisch müssten Backups regelmäßig ebenfalls auf entsprechende Daten untersucht werden, um diese zu löschen. Hier wird der Admin im Normalfall aber nicht mehr ohne juristische Hilfe auskommen, schon um zu erfassen, welche Daten zu löschen sind und welche erhalten bleiben dürfen.

Aufgepasst bei Managementtools

Auch bei Software, die im Büro organisatorischen Zwecken dient, ist erhöhte Vorsicht geboten. Nutzt die Assistenz der Geschäftsführung etwa spezielle Werkzeuge, um Termine der Chefs zu managen – beispielsweise Buchungssoftware für Restaurants –, werden diese schnell eine wahre Goldgrube im Hinblick auf personenbezogene Daten sein. Gerade das ist aber ein hervorragendes Beispiel für Daten mit sehr geringer Halbwertszeit.

Ob man mit der Repräsentantin eines anderen Unternehmens vor zwei Monaten im Café Einstein um 15 Uhr einen Kaffee getrunken

hat oder nicht, mag eine Information sein, die zu speichern legitim ist – etwa aus Gründen der Unternehmensstrategie. In der Mehrzahl der Fälle dürfte ein schneller Kaffee aber nicht von so großem strategischen Interesse sein, dass es legitim wäre, Aufenthaltsorte und -zeiten mehrerer Personen dauerhaft zu speichern. Blöd, wenn solche Daten dann über Jahre und Jahrzehnte erhalten bleiben, weil die Datenbank des Terminverwaltungstools nicht regelmäßig um alte Einträge erleichtert wird. Fällt ein solches Werkzeug bei einer DSGVO-Kontrolle den Prüfern auf, händigt man der Behörde am besten gleich die Zugangsdaten zum Onlinebanking für das Firmenkonto aus, das spart Zeit und Mühe.

Alles noch viel schlimmer: Hardware

Eine Misere, die Administratoren fast gar nicht auf dem Schirm haben, sind Clients und spezielle Geräte für die direkte Nutzung durch Anwender. Wer es etwa extrem praktisch findet, dass sich der Nobel-Kaffeevollautomat im Büro per App steuern lässt und für unterschiedliche Nutzer Geschmacksprofile für den Wunschkaffee anlegen kann, denkt besser noch mal nach. Denn ein Kaffeeprofil, das sich auf dem Gerät einer bestimmten ID oder einer MAC-Adresse zuweisen lässt, ist eindeutig zur jeweiligen Mitarbeiterin oder zum jeweiligen Mitarbeiter zurückverfolgbar. So praktisch das Feature also auch sein mag: Datenschutzrechtlich fährt ein Unternehmen besser, wenn es einen Bogen um derartige Funktionen macht. Denn ganz ehrlich: Wer denkt schon daran, beim Offboarding von Kolleginnen und Kollegen die Kaffeemaschine im Büro auf personenbezogene Daten hin zu untersuchen?

Das Internet of Things klingt verheißungsvoll und bringt Endanwendern nützliche Features, die für Firmen vor dem DSGVO-Hintergrund oft heikel sind (Abb. 3). *Melitta*
Ebenfalls beliebt in diesem Kontext sind Geräte, auf denen einmalig Benutzerzugänge für eine Verbindung zum Hersteller einzurichten sind. Die stellen gerade im Framework für Compliance kleinerer Unternehmen eine Herausforderung dar: Oft legen die Admins, die diese Geräte einrichten, nämlich einen generischen Zugang beim Hersteller an, der etwa ihren codierten Benutzernamen enthält („firmaxyz-maxmeier“). Und selbst wenn der Admin einen generischen Benutzernamen benutzt, kommt oft seine eigene E-Mail-Adresse zum Einsatz. Solche Details lassen sich praktisch nicht mehr auffinden, wenn der Admin das Unternehmen verlässt. Hier liegt es an der Firma, für alle Compliance-Regeln verbindlich vorzugeben, die generische Benutzernamen und die Verwendung von Mailboxen mit generischer Adresse ermöglichen.

Und die Liste lässt sich beliebig fortsetzen. Zeichnet das hauseigene Zugangssystem etwa auf, wann welche Tür geöffnet wird? Kein Problem, werden sich viele Admins denken, solange das Gerät nur aufzeichnet, dass die Tür aufgeht, aber nicht, wer sie öffnet. Anders sieht die Sache allerdings aus, wenn, um Lichter ein- und auszuschalten, im Gebäude auch smarte Bewegungsmelder zum Einsatz kommen, die ebenfalls

Aufzeichnungen führen. Aus der Information, dass um 08:05 Uhr die Türe geöffnet wurde und um 08:08 Uhr im Büro von Frau Müller das Licht anging, lässt sich aber korrelieren, dass diese vermutlich zuvor auch die Tür geöffnet hat – gerade in kleineren Unternehmen und gerade wenn das jeden Tag mit ähnlichen zeitlichen Abständen geschieht. Fans von Big Data geraten ins Schwärmen, Datenschützer hingegen ins Grübeln.

Corona lässt grüßen

Bietet das eigene Unternehmen Zugriff auf den internen Mailserver über das Internet? Gilt in der Firma gar eine BYOD-Philosophie? Wie praktisch! Gerade im Corona-Kontext und unter DSGVO-Aspekten aber alles andere als beruhigend. Denn einerseits gilt: Richtet sich ein Mitarbeiter auf einem privaten Gerät einen Zugang zu seinen Firmenmails ein, fällt dieses sofort unter dasselbe Compliance-Reglement wie alle anderen Geräte der Firma auch. Gerade weil es sich um ein privates Gerät handelt, hat die IT-Abteilung der Firma aber keine Handhabe mehr, zu bestimmen, was mit den Daten passiert. So erstrebenswert der Zugang zur Firmenmail von privaten Geräten aus auch sein mag – aus DSGVO-Sicht verbietet er sich eigentlich.

Dasselbe gilt im Corona-Kontext sogar für die Notebooks, die der Firma gehören und unter deren Compliance-Reglement stehen. Die DSGVO schreibt nämlich explizit vor, dass personenbezogene Daten so zu verarbeiten sind, dass der Zugang durch nicht berechtige Dritte unmöglich ist. Was im Büro noch umsetzbar ist, lässt sich im Homeoffice und innerhalb der eigenen vier Wände kaum rechtssicher implementieren – zumindest dann nicht, wenn kein eigener, abschließbarer Raum zur Verfügung steht. Mal eben die Mails auf dem heimischen Sofa im Wohnzimmer checken scheidet unter diesem Gesichtspunkt eigentlich aus. Dasselbe gilt analog auch für Co-Working-Spaces, in denen der Zugang zum eigenen Arbeitsplatz oft kaum einschränkbar ist.

Unternehmen sind in vielerlei Hinsicht dazu verpflichtet,

bestimmte Daten über einen langen Zeitraum hinweg vorzuhalten. Das ist im DSGVO-Kontext wie beschrieben zunächst kein Problem, weil in diesen Fällen eine andere Rechtsgrundlage besteht. Kommerzielle Lösungen, die für diese Aufgabe zum - Einsatz kommen, verfolgen jedoch das WORM-Prinzip. Sie sind hardware- wie softwareseitig um sämtliche Funktionen erleichtert, die das Modifizieren oder Löschen von Daten ermöglichen. Das wird für viele Unternehmen zum Bumerang, weil sie ihre Archive bisher nach dem Prinzip geführt haben, einfach alles zu archivieren, um sich die mühsame Arbeit des Herausfilterns der tatsächlich benötigten Elemente zu ersparen.

Archivsysteme sind ein Graus

Wer solche WORM-Konstrukte nutzt, wird ad hoc keine technische Lösung finden können, die mit vertretbarem Aufwand auch nur irgendwie realisierbar wäre. Die Deutsche Wohnen führt aus, dass das Gros der im Haus genutzten Software wie beschrieben das Löschen einzelner Dokumente aus Mieterakten aus den eben beschriebenen Gründen nicht beherrscht. Wollte man die Anbieter verpflichten, hier einzelne Teile von Datensätzen aus dem Archiv zu kratzen, müsste die Firma de facto zwei Systeme dieser Art beschäftigen: eines, in dem sie experimentell die Daten löscht, und ein zweites, in das sie dann den gültigen Datensatz überspielt, um wieder den Anforderungen an die eigene Löschpflicht zu genügen.

Archivsysteme wie dieses genügen gesetzlichen Anforderungen und geben WORM-Garantien ab, geraten damit oft aber in Widerspruch zur DSGVO (Abb. 4). *Fujitsu*

Immerhin sieht die DSGVO hier eine Hintertüre vor. Legen Unternehmen überzeugend dar, wieso der zu treibende Aufwand im Spannungsfeld von WORM-Pflichten einerseits und DSGVO-Löschpflicht andererseits zu hoch wäre, haben sie stattdessen die Option, Prozesse zu entwerfen, die verhindern, dass eigentlich zu löschende Daten wieder in Umlauf geraten. Begehren Kunden die Löschung von Datensätzen oder wäre die Löschung nötig, kann man sie dann mit einem entsprechenden Sperrvermerk versehen, der nicht zwingend im selben System hinterlegt sein muss.

Auf Verlangen muss die Firma die entsprechende Prozessdokumentation aber vorlegen können und nachweisen, dass sie in der Praxis tatsächlich zur Anwendung kommt. Und darauf verlassen, dass diese Regelung ewiglich gilt, sollten Unternehmen sich letztlich auch nicht – wer sich des Problems ernsthaft annehmen möchte, muss mit den Entwicklern etwaiger Programme zusammenarbeiten, um Datensätze sinnvoll aufteilbar zu machen. Das bedeutet am Beispiel der Deutsche Wohnen etwa ganz konkret: Die Software für die Verwaltung von Verträgen könnte die ursprünglich eingereichten Dokumente wie Gehaltsnachweise und SCHUFA-Auskünfte von sich aus sofort löschen, sobald ein Mietverhältnis in gegenseitigem Einvernehmen beendet ist. Dass es keine Option ist, das

Problem auszusitzen, zeigt das Beispiel der DW jedenfalls eindrücklich.

Ebbe bei hilfreichen Werkzeugen

Damit ist klar: Moderne IT-Umgebungen strotzen nur so vor Datensenken, die sich für Unternehmen als existenzbedrohend herausstellen können. Da ist es nur verständlich, dass Admins sich Werkzeuge wünschen, die ihnen beim Auffinden der Datentröge helfen und gegebenenfalls Alarm schlagen. Die schlechte Nachricht ist: Solche Tools sind kaum verfügbar. Werkzeuge zur forensischen Analyse beziehen sich eher auf Fälle, in denen ein Einbruch stattgefunden hat und Daten - bereits rausgetragen worden sind. Das ist im DSGVO-Kontext aber nur dann schädlich, wenn die Firma nicht nachweisen kann, dass sie sich an aktuelle technische Standards beim Absichern der eigenen Umgebung gehalten hat.

Dataloss Prevention Tools zäumen das Pferd von hinten auf und sind eher darauf ausgelegt, Prozesse zu installieren, die Datenverlust unwahrscheinlich machen. Das hilft aber nicht in bestehenden Umgebungen, in denen Grundsätze des Datenschutzes über Jahre hinweg nicht zur Anwendung gekommen sind.

Was können Unternehmen also tun? Wie bereits angedeutet, ist die richtige Reaktion auf die DSGVO-Löschpflicht in erster Linie die Einführung passender Prozesse in Kombination mit ausgiebiger Kommunikation mit den eigenen Lieferanten. Standardisierung, Automation und Orchestrierung nehmen viel Angriffsfläche. Überraschenderweise existiert mit der DIN 66398 sogar eine recht praxisorientierte Norm zu diesem Thema (siehe Kasten „Löschkonzepte gemäß DIN 66398“).

Löschkonzepte gemäß DIN 66398

Das DIN hat in der DIN 66398 Empfehlungen als „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ zusammengestellt. Darin finden

sich für das Normungsinstitut ungewöhnlich konkrete Vorgaben zur Vorgehensweise beim Erstellen eines Löschkonzepts.

In einem Blog des Forum-Verlags heißt es, dass demnach Unternehmen eine Reihe von Überlegungen anstellen und Schritte unternehmen sollten (siehe ix.de/z9h2):

- Datenarten, die es im Unternehmen gibt, kategorisieren und deren Aufbewahrungsfristen festlegen.
- Löschregeln für die jeweilige Datengruppe festlegen.
- Konkrete Umsetzungsregeln definieren.
- Die jeweils verantwortlichen Personen für die datenschutzkonforme Umsetzung benennen.
- Prozesse zur Dokumentation ausarbeiten und verbindlich festlegen.

Automation und Orchestrierung

Wer sein Set-up sinnvoll automatisiert und modernen Standards der Systemadministration folgt, minimiert das Risiko von Datensenken auf einzelnen Servern. Überhaupt sollte ein einzelnes System so wenige personenbezogene Daten enthalten wie möglich. Was im Klartext bedeutet: Sämtliche Benutzerzugänge der Systeme kommen aus dem LDAP. Der Prozess des Offboardings sieht Schritte vor, die Daten ehemaliger Kollegen auf Systemen zentralisiert und automatisiert zu entfernen, sofern diese für den Betrieb nicht nötig sind. Logdateien haben in modernen Systemen auf einzelnen Servern nichts mehr zu suchen. Zentralisiertes Logging ist stattdessen das Zauberwort – und ermöglicht es, zentral der DSGVO-Löschpflicht nachzukommen, zum Teil sogar vollständig automatisch.

Was spezielle Software wie Shopsoftware oder Vertragsverwaltungslösungen angeht, hilft nur die enge Kommunikation mit dem Hersteller. Falls der sein Produkt bisher nicht um eine Löschfunktion nach DSGVO-Standards erweitert hat, gilt es, Druck auszuüben, um das zu ändern.

Sich darauf zu verlassen, dass der „Machbarkeitsvorbehalt“ in der DSGVO dauerhaft erhalten bleibt, ist jedenfalls eine fragwürdige Strategie. Hier muss die Software a priori die Möglichkeit bieten, Daten eines Profils zu löschen, ohne dieses gleich vollständig aus dem Bestand zu entfernen.

Den Verheißungen des Internet of Things sollten Unternehmen vom Standpunkt der DSGVO her derzeit widerstehen. Smarte Lichtschalter und schlaue Kaffeemaschinen sind zwar bequem und angenehm. Doch sind sie zentral kaum administrierbar – und sie lassen sich nicht in automatisierte Compliance-Frameworks einbinden und werden so zum potenziellen Datentrog.

Fazit

Es ist eine Krux mit dem Datenschutz: Zu Recht formuliert die DSGVO ein hohes Recht der Menschen an den eigenen Daten, der besonderen Schutzbedürftigkeit dieser Daten und eine Verpflichtung für Daten verarbeitende Unternehmen, hohe Standards zu erfüllen. Für die Admins im Unternehmen geht das aber derzeit mit weitgehend unabwägbaren Risiken einher: In den wenigsten Firmen dürfte wirklich klar sein, wo sich möglicherweise noch alte Bestandsdaten verbergen, die längst den Weg in die ewigen Jagdgründe hätten antreten müssen. Wer jedoch diese Datensätze konsequent suchen und heben möchte, kommt um ein nahezu vollständiges Audit des eigenen Set-ups kaum herum. Und das behebt nur einen Teil der Schwierigkeiten.

Denn verschiedene Softwarelösungen und Archivimplementierungen, ganz gleich, ob in Hard- oder Software umgesetzt, verunmöglichen es, die Löschregeln der DSGVO in Gänze einzuhalten. Hier dürfte zumindest auf absehbare Zeit eine sehr enge Abstimmung mit dem eigenen Rechtsbeistand notwendig sein, um die Grenzen des Erlaubten zu kennen und sich an ihnen entlangzuhangeln. Aber langfristig muss die DSGVO zur Vereinheitlichung und Standardisierung von Set-ups im Rechenzentrum führen, weil sich damit viele Komplikationen im Hinblick auf Datenschutz von vornherein

vermeiden lassen.
(avr@ix.de)

1. Quellen
2. Tobias Haar; Seid sparsam; Löschung personenbezogener Daten; *iX* 11/2020, S. 58
3. Frank Heisel; Ballast abwerfen; Datenlöschen in komplexen Systemlandschaften; *iX* 11/2020, S. 64
4. Weitere Informationen zu Datenempfängern und zur DIN 66398: ix.de/z9h2

Martin Gerhard Loschwitz

ist Cloud Platform Architect bei Drei Austria und beackert dort Themen wie OpenStack, Kubernetes und Ceph.

[/expand]