Kfz-Halterabfragen der Polizei) ist so gegen unbefugtes Mithören geschützt.

Für den Aufbau und Betrieb des BOS-Funksystems ist zentral die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) zuständig. Nutzbar gemacht wird der Digitalfunk für die BOS (z. B. Beschaffung, Freischaltung und Inbetriebnahme von Funkgeräten, technische Betreuung) durch die sog. Autorisierten Stellen von Bund und Ländern, die als „Service-Provider“ auftreten. Bei Beratungs- und Kontrollbesuchen habe ich sowohl die BDBOS als auch die Autorisierte Stelle Bund für den Digitalfunk (AS Bund) aufgesucht, um mich über die konkreten Aufgaben und die Einhaltung des Datenschutzes zu informieren.

Beratungs- und Kontrollbesuche bei der BDBOS

Im Rahmen des BDBOS-Gesetzes (BDBOSG) wurde von der BDBOS ein privates Unternehmen mit dem Aufbau und dem technischen Betrieb der Systemtechnik beauftragt. Da beim Betrieb personenbezogene Daten (Teilnehmernummern) erhoben, gespeichert und verarbeitet werden, musste die BDBOS dafür auch einen Vertrag zur Auftragsdatenverarbeitung schließen, der die Einhaltung des Datenschutzes beim technischen Netzbetrieb sicherstellt. Während diese Beauftragung datenschutzrechtlich nicht zu beanstanden war, halte ich jedoch die pauschale Speicherung sämtlicher Verkehrsdaten für einen Zeitraum von drei Monaten (und im Einzelfall sogar von bis zu 120 Tagen) in Form von Call Data Records (CDR) für unzulässig. Begründet wird die lange Speicherdauer damit, dass im Fehlerfall eine Analyse auch rückwirkend durchgeführt werden können müsse. Aus meiner Sicht rechtfertigt dies jedoch nicht die pauschale Speicherung der durchaus sensiblen Verkehrsdaten ohne konkrete Zweckbindung. In diesem Zusammenhang habe ich auch Bedenken gegen die pauschale Herausgabe dieser Verkehrsdaten an die Autorisierten Stellen des Bundes und der Länder, insbesondere deshalb, weil hier zurzeit keine verbindlichen Dienstanweisungen existieren. Hierzu bin ich weiter im Gespräch mit der BDBOS, um eine datenschutzgerechte Lösung herbeizuführen, die die speziellen Aspekte dieses Funksystems berücksichtigt. Bei meinem letzten Besuch bei der BDBOS ist mir aufgefallen, dass die behördliche Datenschutzbeauftragte nur nach vorheriger Anmeldung Zutritt zum Netzbetriebszentrum des privatwirtschaftlichen Unternehmens erhält, was im Gegensatz zu ihrer Aufsichtspflicht steht. Eine Anpassung an die Vorgaben des BDSG wurde mir hier bereits zugesagt.

Beratungs- und Kontrollbesuche bei der Autorisierten Stelle Bund für den Digitalfunk

Die beim Bundespolizeipräsidium angesiedelte Autorisierte Stelle Bund (AS Bund) ist verantwortlich für die Nutzbarmachung des Digitalfunks für alle Bundesbehörden (auch ressortübergreifend). Zusätzlich trägt die AS Bund die Verantwortung für die Einführung und Nutzung des digitalen Behördenfunks innerhalb der Bundespolizei.

Wie ich bei meiner Kontrolle festgestellt habe, ist durch die technischen Teilnehmernummern des zugrunde liegenden TETRA-Funksystems und die namentliche Erfassung der Beschäftigten bei Ausgabe von Funkgeräten ein Personenbezug möglich und der jeweilige Nutzer bestimmbar. Dieser datenschutzrechtliche Aspekt war den Verantwortlichen vorher nicht klar. Ich habe verdeutlicht, dass es sich deswegen beim Funkverkehr bzw. der Nutzung eines Funkgerätes um einen Umgang mit personenbezogenen Daten handelt, deren Erhebung, Verarbeitung und Nutzung nur zulässig ist, soweit eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Eine entsprechende Rechtsgrundlage konnte mir aber zum Zeitpunkt meines letzten Besuches nicht genannt werden; eine Einwilligungslösung scheidet hier wegen der dienstlichen Verwendung des TK-Systems aus. Hier muss der Gesetzgeber nachbessern.

Ich habe ferner auf die strikte Einhaltung der Zweckbestimmung beim Umgang mit diesen Daten und auf die erforderliche Beteiligung der zuständigen Personalvertretung hingewiesen, da die Verkehrsdaten zur Verhaltens- und Leistungskontrolle der Digitalfunk nutzenden Beschäftigten verwendet werden könnten. Die von mir bereits während meines ersten Besuchs im November 2011 angeregte Dienstanweisung zur Nutzung des Digitalfunks wurde kurz vor meinem zweiten Besuch im November 2012 in Kraft gesetzt. Zu dieser Dienstanweisung habe ich während meines Besuchs im Detail datenschutzrechtliche Änderungs- und Ergänzungsempfehlungen gegeben.

Obwohl der digitale BOS-Funk aufgrund der verschlüsselten Sprachübertragung eindeutige Datenschutzvorteile gegenüber dem analogen BOS-Funk bei der täglichen Anwendung aufweist, müssen auch die datenschutzrechtlichen Anforderungen hier ausreichende Berücksichtigung finden.

6.12 Deutsche Post AG

6.12.1 Konzerndatenschutzrichtlinie der Deutschen Post DHL – ein langer Weg

Die Konzerndatenschutzrichtlinie regelt die datenschutzkonforme Übermittlung von Daten aus der Europäischen Union in Drittstaaten. Die Umsetzung der erteilten Genehmigung dauert länger als erwartet.

In meinem letzten Tätigkeitsbericht (vgl. 23. TB Nr. 10.1) hatte ich über den Abschluss des Genehmigungsverfahrens auf europäischer Ebene berichtet. Spätestens nachdem ich im Februar 2011 die „Deutsche Post DHL Data Privacy Policy (Konzerndatenschutzrichtlinie)“ gebilligt und das Genehmigungsschreiben dem Vorstand überreicht hatte, ging ich von einer zügigen Umsetzung innerhalb des Konzerns aus. Die Deutsche Post DHL (DP-DHL) war nun berechtigt, personenbezogene Daten nach Maßgabe ihrer Data Privacy Policy ins Ausland zu übermitteln, ohne dafür im Einzelfall eine Genehmigung einzuholen. Sie war damit das erste deutsche Unternehmen, dessen verbindliche unternehmensweite Datenschutzregelung (BCR – Binding Corporate Rules) nach einem

umfassenden Konsultationsverfahren zwischen den Datenschutzbehörden der Europäischen Union anerkannt wurde.

Mit meiner Billigung wurde ein (vermeintlich) wesentlicher Schritt auf dem langen Weg bis zur endgültigen Umsetzung der BCR zurückgelegt. Offensichtlich war das unternehmensinterne Verfahren aber so zeitaufwändig, dass mir erst zum Ende des Berichtszeitraums die „Deutsche Post Data Privacy Policy“ in einer Form präsentiert werden konnte, die im Gesamtunternehmen verteilt und dort den geltenden Datenschutzstandard festlegen wird. Im November 2012 hat die letzte Umsetzungsphase, nämlich der Versand der Beitrittserklärungen an die internationalen Konzerngesellschaften, begonnen. Erst im Laufe des Jahres 2013 wird nach den Planungen der DP AG die endgültige Umsetzung der Konzerndatenschutzrichtlinie abgeschlossen sein. Ich bin mir, nicht zuletzt wegen der gegebenen Zusicherung der DP AG, sicher, dass es soweit kommen wird; Prognosen zum zeitlichen Verlauf gebe ich aber keine mehr ab.

6.12.2 Können Packstationen unbesorgt genutzt werden – Kontrollerfahrungen

Der Datenschutz ist gewährleistet, aber Vorsicht bei Phishing-Attacken!

Die überwiegende Zahl der Beschwerden über die Deutsche Post AG (DP AG) betreffen Falschzustellungen, unberechtigte Rücksendungen an den Absender oder die Aufbewahrung von Briefsendungen. Zahlreiche Eingaben, in denen mir Phishing-Attacken bei der Nutzung von Packstationen mitgeteilt wurden, habe ich zum Anlass genommen, mich detailliert vor Ort zu informieren.

Bei den Packstationen handelt es sich um Paketautomaten, an denen Kunden der DP AG Sendungen unabhängig von Öffnungszeiten abholen oder einliefern können. Zur Nutzung dieser Anlage (Ausnahme: Einlieferung von Sendungen) muss sich jeder Kunde zunächst in einem zweistufigen Verfahren registrieren. Dies erfolgt im ersten Schritt durch Ausfüllen eines Online-Registrierungsformulars, in dem u. a. die E-Mail-Adresse und die Mobilrufnummer anzugeben sind; über diese Kontaktkanäle wird der Kunde über abholbereite Sendungen informiert. Im zweiten Schritt werden diese Angaben im Postidentverfahren verifiziert, danach erhält der Kunde persönlich die Unterlagen zur Nutzung der Packstationen („Begrüßungsset“).

Die Petenten berichteten, dass sie per E-Mail um Herausgabe ihrer Authentisierungsdaten (Postnummer und PIN) gebeten wurden. Diese E-Mails erweckten den Anschein, als würde es sich um Anschreiben der DP AG handeln. Auf diesem Weg versuchten unbekannte Dritte, illegal Zugriff auf die in den Packstationen lagernden Sendungen zu erhalten.

Die DP AG teilte mir auf meine Nachfrage mit, sie sei über diese Angriffe und Manipulationsversuche informiert und habe als Gegenmaßnahme Hinweise auf mögliche Phishing-Angriffe und zum sicheren Umgang mit den Zugangsdaten im Begrüßungsset aufgenommen. Der Kunde werde eindeutig darauf hingewiesen, dass die zur Warenabholung notwendigen Daten auf keinen Fall weitergegeben werden dürften. Zur Eindämmung der Phishing-Problematik gründete die DP AG zudem ein sog. Anti-Phishing-Response-Team, das Angriffe analysieren und die Sperrung der entsprechenden Internetseiten veranlassen soll. Weiter wurde das Authentisierungsverfahren zur Warenabholung mittels Postnummer und PIN umgestellt. Nun ist zusätzlich seit dem 2. Quartal 2011 eine Magnetstreifenkarte zur Abholung notwendig.

Seit November 2012 wurde die Magnetstreifenkarte durch eine mobile TAN (mTAN) ersetzt, die der Kunde per SMS erhält. Da die mTAN eine transaktionsbezogene Nummer mit begrenzter Gültigkeit ist, wird so ein potentieller Missbrauch zusätzlich erschwert. Aufgrund dieser Sicherheitsmechanismen greifen Phishing-Mails nicht mehr.

Auch wenn keine hundertprozentige Sicherheit gewährt werden kann, sehe ich das aktuelle Verfahren beim Abholen von Sendungen an den Packstationen mittels PIN und mTAN als datenschutzkonform an. Auch die Prüfung der Identität bei der Anmeldung zu diesem Verfahren entspricht den datenschutzrechtlichen Vorgaben.

Aufgrund weiterer Eingaben habe ich mir darüber hinaus auch in einem Verteilzentrum und in einem Zustellstützpunkt einen persönlichen Eindruck davon verschafft, ob und wie die datenschutzrechtlichen Vorgaben dort eingehalten werden. Trotz umfangreicher Schulungsmaßnahmen, die von Qualitätskontrollen bei der Zustellung begleitet werden, lassen sich Fehler beim Umgang mit Paket– und Briefsendungen leider nicht immer vermeiden. Mir ist durchaus bewusst, dass dies für den Betroffenen mit viel Ärger und manchmal sogar mit Nachteilen verbunden sein kann, aber auch hier gilt der Grundsatz „wo gehobelt wird, da fallen Späne“. Es ist jedoch zu berücksichtigen, dass sich diese unerfreulichen Versäumnisse der Anzahl nach im unteren Promillebereich bewegen.

Insgesamt bleibt festzustellen, dass sich die Dienstleistungen der DP AG auf einem hohen Datenschutz- und Qualitätsniveau bewegen. Die mir bekannt gewordenen Fehler mit Datenschutzrelevanz sind durchweg auf einzelnes menschliches Fehlverhalten zurückzuführen und keinesfalls durch fehlerhafte Systemprozesse bedingt. Nach meiner Einschätzung kann der Datenschutz hier nur durch noch bessere Schulungs- und Sensibilisierungsmaßnahmen weiter verbessert werden.

6.13 Hohes Datenschutzniveau bei den Postdienstleistern

Auf dem Markt der Postdienstleister haben sich neben der Deutschen Post AG eine Reihe weiterer Lizenznehmer etabliert; dabei handelt es sich überwiegend um kleine und mittlere Unternehmen, die insbesondere auf regionalen Märkten tätig sind.

Auch zu diesen Unternehmen haben mich Eingaben erreicht, die in etwa die gleichen Probleme wie beim „gelben Bruder“ zum Gegenstand hatten. Thematisiert