

Best-Practice-Modell aus Österreich

Vertreter von österreichischen Telekom-Anbietern und Behörden präsentierten bei Europol die „Durchlaufstelle“ als Best-Practice-Modell für den sicheren Austausch sensibler Daten.

Der sichere und transparente Datenaustausch zwischen Telekom-Anbietern und Behörden ist eine Herausforderung für die beteiligten Institutionen. Es geht nicht nur darum, dass genau jene Daten übermittelt werden, die von der anfragenden Stelle benötigt werden, sondern die Daten müssen auch so aufbereitet sein, dass sie von dieser verarbeitet werden können. Darüber hinaus muss die Übermittlung verschlüsselt und signiert sein, um sicherzustellen, dass nur legitimierte Personen die Daten entschlüsseln und einsehen können. Ein Fehler in einem derartigen System bedeutet für die Rechtsdurchsetzungsbehörden im schlimmsten Fall keine oder fehlerhafte Informationen, für die Telekom-Anbieter zieht ein potenzieller Fehler neben Sanktionen einen Image-Verlust in der Öffentlichkeit nach sich.

Systeme, die diesen Ansprüchen genügen, sind meist komplex und benötigen hohe Investitionen in der Implementierung und im Betrieb. Es gibt Beispiele für den Datenaustausch zwischen Behörden und Telekom-Anbietern, die den Anforderungen nicht gerecht werden. Ein solches Beispiel wurde bei einer Europol-Veranstaltung von einer Polizeibehörde eines EU-Landes vorgestellt. URLs zu kinderpornografischen Inhalten, die von den Providern nach nationalem Recht gesperrt werden müssen, werden als Tabelle in einer unverschlüsselten E-Mail über eine Mailingliste an die Telekom-Anbieter übermittelt. Diese Lösung wurde als „kostengünstige und einfache Methode für den Datenaustausch“ bezeichnet.

Bei den Vertretern der Telekom-Industrie löste dieses Beispiel Unverständnis aus und Europol musste sich die Kritik gefallen lassen, warum einer solchen mangelhaften Lösung eine Bühne geboten werde. Dadurch werde das Vertrauen der Internetbranche und der Öffentlichkeit in die technische Kompetenz bzw. das datenschutzrechtliche Grundverständnis der Rechtsdurchsetzungsbehörden europaweit untergraben.

Präsentation der „Durchlaufstelle“. Die Kritik wurde vom Veranstalter zwar



Maximilian Schubert (ISPA): „Durchlaufstelle“ als Best-Practice-Modell für den sicheren Datenaustausch.

ISPA

Dachorganisation der Internetwirtschaft

Die Interessensvertretung *Internet Service Providers Austria (ISPA)* ist die Dachorganisation der Internetwirtschaft, besteht seit 1997 und stellt den mehr als 200 Mitgliedern Expertise und Know-how zur Verfügung, auch in rechtlichen Angelegenheiten. Es werden Stellungnahmen zu Gesetzesentwürfen abgegeben, Mustervorlagen für *Allgemeine Geschäftsbedingungen (AGB)* erarbeitet und Sicherheitskonzepte entworfen. Mitglieder können sich kostenlos an der *ISPA-Academy* weiterbilden. Der Verein veranstaltet das *ISPA-Forum* und der *Internet Summit Austria*. ISPA betreibt eine Stelle, bei der Kinderpornografie und nationalsozialistische Inhalte im Internet gemeldet werden können („Stopline“). Angeboten wird auch Informationsmaterial zur Förderung der Online-Medienkompetenz von Kindern und Jugendlichen.

www.ispa.at

zur Kenntnis genommen, die Vertreter der Telekom-Industrie bekamen aber das Feedback, dass ihre kritische Rückmeldung die einzig negative gewesen sei. Viele nationale Behördenvertreter hätten sich sehr interessiert an dieser einfachen und kostengünstigen Möglichkeit des Datenaustausches gezeigt. Vertretern der Interessensvertretung *Internet Service Providers Austria (ISPA)* wurde aber die Möglichkeit eingeräumt, in einer Europol-Arbeitsgruppe die österreichische Lösung des sicheren Datenaustausches zwischen Providern und Behörden vorzustellen.

ISPA-Generalsekretär Dr. Maximilian Schubert präsentierte Ende November 2016 mit Vertretern des österreichischen Bundesministeriums für Inneres (BMI), des Competence-Centers Telekommunikationsüberwachung, des Bundeskriminalamts, der TU Wien und eines österreichischen Providers bei einem Treffen der Europol-Expertenarbeitsgruppe *Advisory Group on Communication Providers*, das Modell der österreichischen „Durchlaufstelle“. Die *Advisory Group on Communication Providers* ist beim Europäischen Zentrum zur Bekämpfung der Cyber-Kriminalität (*European Cybercrime Centre – EC3*) in Den Haag angesiedelt.

Entstehungsgeschichte. Die „Durchlaufstelle“ wurde im Zuge der Einführung der Vorratsdatenspeicherung durch ein Grundrechtsforschungsinstitut in Zusammenarbeit mit der TU Wien, dem BMI und anderen betroffenen Behörden sowie den österreichischen Internet Providern entwickelt. Es handelt sich um ein elektronisches Postfachsystem zur sicheren Abwicklung von Anfragen. Das System stellt die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicher. Alle Beteiligten sind über einen verschlüsselten Übertragungskanal angebunden.

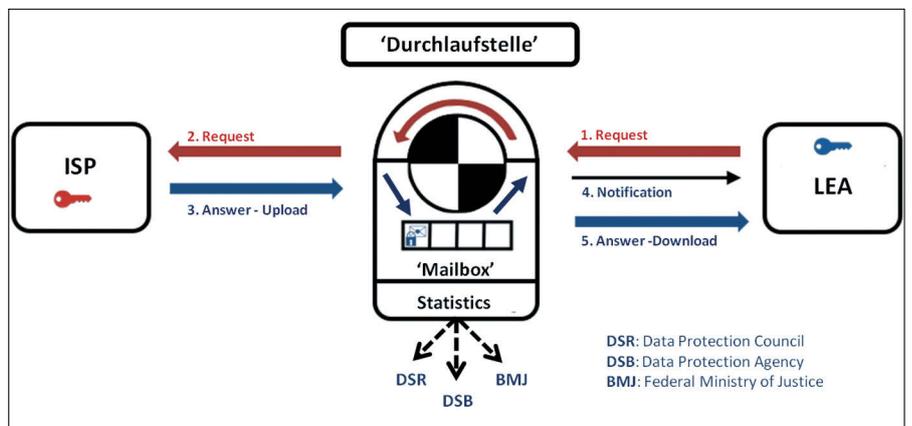
Die „Durchlaufstelle“ wird nach Wegfall der Vorratsdatenspeicherung weiterverwendet, um Behörden Auskunft zu geben über beim Betreiber – etwa für Verrechnungszwecke – vorhandene Verkehrsdaten.



Europol-Zentrale in Den Haag: Präsentation der „Durchlaufstelle“ für den Datenaustausch zwischen Providern und Behörden.

Bei der Präsentation bei Europol zeigten sich die Vertreter der Industrie und Behörden nicht nur vom gebotenen Level an Sicherheit und Transparenz angetan. Auf Wohlwollen stieß auch der Umstand, dass der Betrieb der „Durchlaufstelle“ bei allen Beteiligten nur minimale Voraussetzungen erfordert – es ist lediglich ein aktueller Browser notwendig. Die Kosten belaufen sich auf einen Bruchteil jener von vergleichbaren proprietären Systemen. Die erhebliche Beschleunigung bei der Abwicklung der Anfragen, die durch die Einführung des Systems in Österreich erreicht werden konnte, wurde positiv aufgenommen. Früher erfolgten Anfragen oftmals via Fax und mussten mehrfach abgetippt werden.

Auf Interesse stieß auch der Prozess, der in Österreich zur gemeinsamen Erarbeitung dieses Systems geführt hatte. Österreich war bei der Umsetzung der Vorratsdatenspeicherung säumig, was im Sommer 2013 zur Einleitung eines Vertragsverletzungsverfahrens durch die Europäische Union geführt hat. Um die technischen Voraussetzungen zum Datenaustausch schnellstmöglich zu implementieren und Strafzahlungen der



„Durchlaufstelle“: Verschlüsselter und signierter Datenaustausch.

Republik zu vermeiden, waren Behörden und Provider aufeinander angewiesen. Es folgten Gesprächsrunden mit Vertreterinnen und Vertretern von Behörden und Providern, aber auch der Forschung, in denen der Bedarf der Behörden und die technischen Gegebenheiten der Provider sowie die grundrechtlichen Vorgaben diskutiert wurden.

Unter der Leitung eines Grundrechtsinstituts kam es rasch zu einer tragfähigen Lösung, die den Bedürfnissen aller Seiten entspricht. Zwar sind die Sichtweisen von Behörden und Be-

treibern noch immer unterschiedlich, beide Seiten tauschen sich aber laufend aus und arbeiten gemeinsam an Verbesserungen und neuen Lösungen.

Nach der Präsentation der „Durchlaufstelle“ in Den Haag und der anschließenden Diskussion mit Vertretern von Europol und Experten der größten europäischen Telekommunikationsanbieter wurde vereinbart, die Eckpunkte der österreichischen Lösung in ein „White Paper“ der Europol zum Datenaustausch zwischen Providern und Behörden einfließen zu lassen. *M. S.*