datenschutz-berater.de

45. Jahrgang

DSB 06/2021

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Stichwort des Monats

Datenschutz im Fokus

Aktuelles aus den Aufsichtsbehörden

Rechtsprechung

ISSN 0170-7256

dfv Mediengruppe

Jannik Krone

Kritik an unverschlüsselten Faxen: Es ist eine Einstellungsfrage

Das „Fax-Verbot" im 3. Tätigkeitsbericht der Bremer Landesdatenschutzbeauftragten (siehe dort S. 33) und dem Urteil des OVG Lüneburg v. 22.07.2020 – 11 LA 104/19 wird auf eine fehlende Vertraulichkeit von Faxen gestützt. Faxe seien wegen der Übertragung mittels Voice-over-IP wie unverschlüsselte E-Mails und daher unsicher. Folglich dürfte eigentlich dasselbe auch für die Telefonie gelten. Abgesehen von Fragen der Zuständigkeit der Datenschutzaufsichtsbehörde für eine solche Einschätzung, verkennt die Einschätzung die technische Entwicklung der letzten Jahre. Wie nachfolgend dargelegt, kann mit sehr einfachen Schritten eine Transportverschlüsselung auch bei VoIP-basierten Faxen und Telefonaten erreicht werden.

Hintergrund

Seit der Einführung von VoIP-Anschlüssen erfolgt die Übertragung von Telefonie und Fax nicht mehr Leitungs- sondern Paketbasiert über Datenverbindungen. Diese Datenverbindung kann (muss aber nicht) über das Internet erfolgen. Folglich ergeben sich für Telefonie- oder Faxverbindungen, die das gesicherte Netzbetreibernetz verlassen und über das Internet geroutet werden, dieselben Probleme wie bei anderen Datenverbindungen über das Internet. Insbesondere die Abhörproblematik durch Dritte steht im Raum.

Die Diskussion weist zwar einige Parallelen zum Thema Verschlüsselungsstufen bei E-Mails (Transport vs. Ende-zu-Ende-Verschlüsselung) auf (siehe dazu auch Schnebbe, DSB 2020, 297 ff.; Petrlic, DSB 2021, 88 ff.). Allerdings besteht bei Fax und Telefonie gegenüber E-Mail eine Besonderheit: Faxe und Telefonie sind Universaldienste und unterfallen damit als Telekommunikation dem Telekommunikationsgesetz (TKG). Anders als E-Mail-Netzbetreiber sind Anbieter von Telekommunikationsnetzen oder öffentlich zugänglicher Telekommunikationsdienste (mithin für Fax und Telefon) bei der Bundesnetzagentur (BNetzA) registriert und unterliegen ihrer Aufsicht und Sicherheitsanforderungen.

Zuständigkeit

Die Zuständigkeitsfragen sind keine Kühr, sondern für die Praxis bei der Frage entscheiden, welchen Guidelines oder Meinungen durch Unternehmen zu folgen ist.

Das Verhältnis von Datenschutz und TK-Recht

Das Verhältnis von Telekommunikations- und Datenschutzrecht ist kompliziert. Bereits für die Bestimmung der zuständigen Behörde ist zu unterscheiden, ob die Datenverarbeitung Telekommunikation ist – dann gilt das TKG – oder nicht – dann gelten das BDSG bzw. die Landesdatenschutzgesetze.

Die Zuständigkeit für Universaldienste ist (anders als OTT-Dienste wie Messenger-Apps) (nach bisherigem Recht) nur nach dem TKG zu beurteilen.

Materiell-rechtlich untersagt Art. 95 DSGVO es über die ePrivacy-RL hinausgehende Anforderungen zu stellen. Bei Universaldiensten ist für die Feststellung des relevanten datenschutzrechtlichen Maßstabs daher zunächst zu prüfen, ob die ePrivacy-RL spezielle Regelungen enthält. Dies tut die ePrivacy-RL z. B. für die technischen Schutzstandards in Art. 4, für die Vertraulichkeit in Art. 5 und eine Ausnahme für staatliche Abhörmaßnahmen in Art. 15 Abs. 1. Soweit diese Vorschriften der ePrivacy-RL Anwendung finden, kann nach Art. 95 DSGVO kein höherer Schutzstandard gefordert werden.

Keine Landeszuständigkeit für die Festlegung des technischen Schutzniveaus

Die Zuständigkeit im TKG ist insgesamt etwas diffus geregelt. Für die technische Sicherheitsanforderungen trifft § 109 Abs. 6 TKG allerdings eine sehr eindeutige Aussage, wonach die BNetzA – in Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) – einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen erstellt. Dieser Sicherheitskatalog legt die erforderlichen Sicherheitsmaßnahmen für Telekommunikationsdienste und -anbieter fest. § 109 TKG dient der Umsetzung von Art. 4 ePrivacy-RL. Schärfere Anforderungen können daher gemäß Art. 95 DSVGO nicht außerhalb des TKG auf Art. 32 DSVGO gestützt werden.

Keine Landeszuständigkeit für Überwachung von Netzbetreibern

Nach § 115 Abs. 1 TKG sind sowohl BNetzA als auch BfDI, in einer Art überschneidenden Kompetenz, jeweils für die Kontrolle der technischen Schutzmaßnahmen des TKG zuständig. Maßnahmen kann allerdings nur die BNetzA ergreifen. Der BfDI kann nur gegenüber der BNetzA beanstanden. Auch wenn der BfDI in seinem 2020er Tätigkeitsbericht diese Situation als unzufriedenstellend bezeichnet, ist sie nach wie vor die geltende Rechtslage. Unstreitig ist weiter, dass die Landesdatenschutzbeauftragten gemäß

§ 115 Abs. 4 TKG für die Überwachung von Netzbetreiber unzuständig sind.

Zwischenfazit

Über den Umweg des Art. 32 DSGVO kann von Netzbetreibern gemäß Art. 95 DSGVO kein höheres Schutzniveau verlangt werden, als es nach der ePrivacy-RL definiert ist. Das Schutzniveau nach der ePrivacy-RL festzulegen, obliegt in Deutschland der Trojka aus BNetzA, BSI und BfDI. Das TKG entzieht damit den Landesdatenschutzbehörden nicht nur die Kontrolle, sondern auch die Definition des Schutzstandards. Für spezielle Landesanforderungen fehlt den Landesdatenschutzbehörden eine Rechtsgrundlage.

Sicherheit von Faxen und Telefonie

Generell ist zunächst die Frage, welches Schutzniveau die BNetzA von den Netzbetreibern nach § 109 TKG fordert.

Was heißt eigentlich Sicherheit?

Dazu hat die BNetzA hat in Zusammenarbeit mit BSI und BfDI den am 23. Dezember 2020 in Kraft getretenen Sicherheitskatalog in Version 2.0 veröffentlicht, der die Anforderung ausgestaltet. Anlage 1 des Sicherheitskatalogs regelt die Anforderungen an TK-Diensteanbieter mit IP-Infrastruktur und schreibt im für VoIP relevante Teil „3.3.2 Vertraulichkeit der Kommunikation" vor: „Ergänzend zu Abschnitt 2.1.1 sollten im Rahmen des technisch möglichen und wirtschaftlich vertretbaren VoIP-Daten sowohl bei der Übertragung zwischen Netzbetreiber-Netzen als auch – sofern das CPE [das Endgerät] des Kunden die technischen Voraussetzungen dafür bietet – zwischen Kunden-CPE und SBC [den Übergangspunkt von der Kundenleitung in das Netz] des Netzbetreibers verschlüsselt übertragen werden." Das Wort „sollten" an dieser Stelle ist wichtig, weil die Maßnahme anders als eine „Muss"-Vorschrift eben nicht zwingend ist. Die Umsetzungspflicht des neuen Sicherheitskatalogs endet 1 Jahr nach Inkrafttreten, mithin am 23. Dezember 2021.

Die Vorgängerversion 1.1 vom 7. Januar 2016 sah keine entsprechende Pflicht vor. Es gab keine für VoIP-spezifische Anlage 1 und unter Nr. 8.1 und Nr. 8.2.13 war nur abstrakt eine Verschlüsselung nach dem „Stand der Technik" festgelegt.

Auch das BSI gibt im aktuellen IT-Grundschutz Modul NET.4.2, für VoIP-Anwendungen mit hohen Sicherheitsanforderungen, die Verschlüsselung nur als „soll" und nicht als „muss" an (Grundschutzstand Februar 2021, Ziff. NET.4.2.A15).

Anders als die Bremer Landesbehörde kommen die zuständigen Behörden in ihrem erst im letzten Jahr überarbeiteten und verabschiedeten Sicherheitskatalog zum Ergebnis, dass weder eine Ende-zu-Ende-Verschlüsselung (E2E-Verschlüsselung) erforderlich wäre noch, dass eine durchgängige Transportverschlüsselung vorherrschen muss. Kunden müssen also nicht ausschließlich verschlüsselt mit den Diensten kommunizieren.

Stand der Technik

Zweck der Sicherheitsmaßnahmen der Netzbetreiber ist der Schutz vor unbefugtem Zugriff (Art. 4 Abs. 1a zweiter Spiegelstrich ePrivacy-RL) unter Berücksichtigung des Standes der Technik, der Kosten der Durchführung in angesichts des bestehenden Risikos (Art. 4 Abs. 1 ePrivacy-RL). Der Schutz vor unbefugtem Zugriff kann durch Verschlüsselung sichergestellt werden, aber auch anderen Maßnahmen wie eine besondere physische Sicherung der Leitung, etwa in einem Rechenzentrum oder die Übertragung über ein solches gesondert gesichertes Netz kommen in Betracht. So leitet z. B. die Deutsche Telekom ihre VoIP-Verbindungen durch ein eigenes getrenntes Netz und nicht über das Internet.

Der Sicherheitskatalog der BNetzA spiegelt den Stand der Telekommunikationstechnik wider. Die Transportverschlüsselung als bloße Soll-Vorschrift mag in Anbetracht der Diskussion zur Transportverschlüsselung bei E-Mails oder HTTPS-Verbindungen überraschen (siehe dazu auch Schnebbe, DSB 2020, 297 ff.; Petrlic, DSB 2021, 88 ff.). Es darf aber nicht vergessen werden, dass für Echtzeitkommunikation wie VoIP andere Protokolle eingesetzt werden. Bei VoIP wird neben SIP für die eigentlichen Gesprächsdaten das verbindungslose RTP genutzt, unter anderem um die Latenz möglichst gering zu halten. Der Standard für verschlüsselte VoIP-Gespräche ist SRTP. Der Einsatz von SRTP wird im BSI-Grundschutz NET.4.2.A15 für Verbindungen ebenfalls nur mit „soll" empfohlen, nicht als „muss" vorgeschrieben. Zu Schlüsselverwaltung empfiehlt das BSI MIKEY vor ZRTP (siehe dazu BSI-TR-02102-1). Es fehlt jedoch für SRTP derzeit an einer dem HTTPS vergleichbaren Public-Key-Infrastruktur (PKI) für einen Schlüsselaustausch für Endnutzer. Der ohne PKI oder pre-shared-Keys funktionierende ZRTP-Standard findet sich nur in vereinzelten Softwareangeboten, ist in Endgeräten überhaupt nicht verbreitet und erfordert außerdem einen verbalen Abgleich eines Sicherheitscodes durch die Endnutzer.

Aufgrund des verbreiteten Fehlens von Voraussetzungen ist es folgerichtig, dass die BNetzA zunächst die Verschlüsselung zwischen den Betreibernetzen (nur) als „soll" fordert. Dabei handelt es sich um einen überschaubaren Adressatenkreis, bei dem sich Verschlüsselung auch ohne etabliertes Schlüsselmanagement handhaben lässt. Aufgrund der (derzeit) kaum vorhandenen Unterstützung bei den in der Praxis eingesetzten Endgeräten, ginge eine allgemeine Pflicht zur Transportverschlüsselung über den Stand der Technik hinaus und wäre kaum durchführbar.

Große Teile der Endnutzer müssten andernfalls vom Netz getrennt werden.

Derzeit läuft in Deutschland auf Netzbetreiberseite das Ausrollen von SRTP für die Transportverschlüsselung zwischen Kunden-CPE und Netzbetreiber-SBC. So bieten die deutsche Telekom (seit ca. Oktober 2020) SRTP-Transportverschlüsselung sowohl bei Trunking-Anschlüssen als auch an normalen Endkundenanschlüssen an, gleiches gilt für die Anbieter easybell und dus.net für ihre Kunden. Die Unterstützung auf VoIP-Routern wird derzeit von einigen Anbietern (z. B. AVM) und auf VoIP-Telefonen (z. B. Snom) per Softwareupdate ausgerollt. Von einer flächendeckenden Unterstützung kann aber derzeit noch nicht gesprochen werden.

Anzumerken ist, dass SRTP nur auf Sprachverbindungen Anwendung findet. Sofern Faxe nicht als analoge Faxe (z. B. G3-Klasse) am VoIP-Anschluss betrieben werden, sondern mittels dem T.38-Standard, kann dies dazu führen, dass ein unverschlüsselter Transfer erfolgt. T.38 kennt keine Verschlüsselung. Hervorzuheben ist daher, dass die Telekom, beim Einsatz von T.38 zwar keine Verschlüsselung unterstützt, allerdings dann ein Fallback auf G.711 mit aktivierter Verschlüsselung erfolgt. (Schnittstellendefinition der Telekom: https://ogy.de/Telekom-1TR119 S. 20)

Eine darüberhinausgehende E2E-Verschlüsselung scheitert bereits daran, dass der Netzbetreiber die VoIP-Verbindung im Zweifel an einen Nicht-VoIP-Empfänger verbinden muss, etwa einen Mobilfunk-, analogen oder ISDN-Anschluss. Dort existiert keine E2E-Verschlüsselung. Der Netzbetreiber muss zur Konvertierung im Media Gateway die Inhalte im Klartext vorliegen haben. E2E-Verschlüsselung kommt daher nur bei beidseitiger VoIP-Nutzung in Frage. Die Information, ob eine Telefonnummer zu einem VoIP-Anschluss gehört oder nicht, hat aber – mangels öffentlichen ENUM-Verzeichnisses – nur der jeweilige TK-Anbieter. Mangels eines öffentlichen PKI kann ohne Überprüfung durch den Nutzer nicht sichergestellt werden, dass nicht ein gefälschter Schlüssel übermittelt wurde. Für eine E2E-verschlüsselte VoIP-Verbindung muss daher dem TK-Anbieter vertraut werden, dass er korrekte Angaben und den richtigen Schlüssel (vgl. ETSI TR 102 478 v. 1.1.1, S. 27) mitteilt.

ZRTP als Alternative für einen vertrauenslosen Schlüsselaustausch setzt auf einen manuellen Abgleich des Nutzers. Anders als beim Einsatz von S/MIME oder PGP bei E-Mails können dort keine Gateways zur Überprüfung eingesetzt werden, sondern die Gesprächsteilnehmer müssen sich gegenseitig den aktuellen Sicherheitscode vorlesen.

Die beteiligten TK-Anbieter und Geräte müssten die SRTP-Pakete auch netzübergreifend weiterleiten, was nicht sichergestellt ist, da SRTP ein Profil von RTP ist und anders als bei E-Mails nicht nur ein „verschlüsselter Anhang".

Maßnahmen zur E2E-Verschlüsselung wären allerdings zum Schutz vor böswilligen TK-Anbietern erforderlich, nicht zum Schutz des unerlaubten Abhörens bis zum TK-Anbieter. TK-Anbieter unterliegen – wie oben dargelegt – einer erheblichen Regulierung und Aufsicht. Sie müssen in diesem Rahmen sogar staatliche Überwachungsmaßnahmen ausführen (vgl. § 110 TKG und die TKÜV), unverschlüsselte Mobilfunk und ISDN-Gespräche anbieten, etc. Der Sicherheitsgewinn durch das Ausrollen von E2E-Verschlüsselung im TK-Bereich ist daher marginal. Demgegenüber müsste für E2E-Verschlüsselung die gesamte TK-Infrastruktur umgerüstet werden, angefangen mit dem Ausrollen einer PKI, eines öffentlichen ENUMs, Austausch von Endgeräten und Nutzertraining. Überdies hätte das den Nebeneffekt, dass staatliche Abhörmaßnahmen (wenn das Ziel Schutz vor dem TK-Anbieter selbst ist) entgegen § 110 Abs. 1 TKG, §§ 3, 5 TKÜV nicht mehr möglich wären. Abhörmaßnahmen sind allerdings nach Art. 15 Abs. 1 ePrivacy-RL eine zulässige Beschränkung der Vertraulichkeit und vom BVerfG im Posteo-Beschluss (v. 20.12.2018 – 2 BvR 2377/16 Rn. 50) ausdrücklich als legitim bestätigt worden.

Zwischenfazit

Innerhalb des Anbieternetzes sind Inhalte durch gesonderte Maßnahmen gegen unbefugte Kenntnisnahme gesichert. Der Verkehr zwischen Kunde und TK-Anbieter ist bei Transportverschlüsselung abgesichert. Die Transportverschlüsselung ist – mangels Verbreitung – in der Telekommunikation noch nicht Stand der Technik. Selbst die Umsetzung der Soll-Pflicht für die Transportverschlüsselung muss erst mit Ablauf der Umsetzungsfrist des neuen Sicherheitskatalogs der BNetzA erfolgen. E2E-Verschlüsselung ist weit vom Stand der Technik entfernt und mit nur marginalen Sicherheitsgewinn verbunden, hat dafür aber Kollateralschäden bei TK-Überwachung. Derartige Forderungen übersteigen daher den nach Art. 95 DSGVO zulässigen Rahmen.

Sicherheit ist Einstellungssache – Umsetzung

Die Kritik an der die Sicherheit der Verbindung rührt daher, dass, wie oben dargestellt, die VoIP-Verbindung auf dem Weg vom Kunden zum Netzbetreiber ungeschützt über das Internet bzw. außerhalb eines geschützten Netzbetreibernetzes laufen. Diesem Problem kann durch das nunmehr von den Netzbetreibern begonnen Angebot einer Transportwegverschlüsselung begegnet werden.

Die Verschlüsselung ist bei aktuellen Routern sehr einfach zu aktivieren (vom Autor auf einer handelsüblichen Fritz. B.ox 7590 zusammen mit einem Telekomanschluss getestet). Es kostet buchstäblich einen Klick in den Rou-

ter-Einstellungen bei der Telefonnummer den Haken „Verschlüsselte Telefonie aktivieren“ zu klicken.

Um sicherzugehen, dass auch Fax-Verbindungen verschlüsselt sind, sollte auf den Einsatz von T.38 verzichtet werden. Die hier beschriebene Transportverschlüsselung mittels SRTP löst dann die Problematik sowohl für Faxe als auch für Telefonie.

Beurteilung auf der Seite der Endteilnehmer

Da Unternehmen keine Telekommunikationsanbieter, sondern -teilnehmer sind, könnten die Landesbehörden für die Beurteilung der Sicherheit von Telekommunikationsdiensten auf ihrer Seite zuständig sein.

Keine Zuständigkeit für die Beurteilung der Sicherheit auf der Seite der Endteilnehmer

Gegen eine gesonderte Zuständigkeit der Landesdatenschutzbehörden spricht die ausschließliche Gesetzgebungskompetenz des Bundes für Telekommunikation in Art. 73 Abs. 1 Nr. 7 GG. Der Bund regelt z. B. in § 41b TKG welche Telekommunikationsendeinrichtungen an öffentlichen Telekommunikationsnetzen betrieben werden dürfen. Die BNetzA ist sowohl für die Standardisierung der Sicherheitsanforderungen in TK-Netzen als auch der Umsetzung und Einhaltung der TKÜV verantwortlich. Diese einheitliche Zuständigkeit würde unterlaufen, wenn die Landesbehörden eigene Anforderungen stellen dürften, die sogar evtl. zur Aushebelung der TKÜV führten. Die Frage der Verschlüsselung ist – wie oben dargelegt – eine Frage der Schnittstellenspezifikation und damit TK-Recht.

Dieser nationalen (föderalen) Zuständigkeitsverteilung folgt unionsrechtlich die Zuständigkeitsverteilung für die Durchsetzung der ePrivacy-RL und der DSGVO: Der EDSA äußerte in seiner Stellungnahme 5/2019, dass die Zuständigkeit für die Durchsetzung der ePrivacy-RL und der DSGVO nicht auseinanderfallen solle (Rn. 63 ff.). Tut sie dies, wie in Deutschland, darf die Datenschutzbehörde nur den ihnen zugewiesenen DSGVO-Teil untersuchen (Rn. 68). Der EDSA stellt weiter fest, dass die Datenschutzbehörden nur dann Datenverarbeitungsvorgänge im Bereich des ePrivacy-Rechts untersuchen dürften, wenn das nationale Recht ihnen entsprechend die Zuständigkeit übertrage (Rn. 86). Die Frage der Sicherheit auch auf Endkundenseite regelt allerdings bereits das BNetzA-Konzept als bloße Soll-Vorschrift (siehe oben Wortlaut des BNetzA-Sicherheitskonzepts).

Deutlich wird diese Zuständigkeitsverteilung des Art. 95 DSGVO auch aus ErwGr. 173 zur DSGVO, wonach die DSGVO nicht auf Fragen Anwendung finden soll, die bereits in der ePrivacy-RL geregelt sind und deren Regelungen dasselbe Ziel verfolgen. Sowohl Art. 4 Abs. 1a zweiter Spiegelstrich ePrivacy-R als auch Art. 32 Abs. 1 lit. b, 5 Abs. 1 lit. f DSGVO regeln die Frage der Vertraulichkeit und verfolgen das Ziel vor unberechtigtem Zugriff zu schützen. Da die ePrivacy-RL eine zielgleiche Regelung trifft, besteht kein Raum, dass eine Landesdatenschutzbehörde eine eigene, nur auf die DSGVO gestützte Sicherheitsanforderung in Bezug auf TK-Nutzung schafft. Andernfalls würden Netzbetreibern entgegen Art. 95 DSGVO zusätzliche Pflichten auferlegt.

Die BNetzA definiert den Stand der Technik

Selbst wenn dieses Argument nicht zufrieden stellen sollte: Der Stand der Technik wurde unter Beteiligung von drei Bundesbehörden definiert (s. o.). Diese gehen bei einer Verschlüsselung im TK-Bereich nur von einer „soll“-Vorschrift aus (vgl. oben BSI-Grundschutz). Fordert man dennoch über das Datenschutzrecht eine Verschlüsselung zum Netzbetreiber (siehe oben bzgl. Probleme der E2E-Verschlüsselung), wäre das zumindest mittels SRTP möglich.

Die Landesdatenschutzbehörden sollten bei den Behörden aufräumen

Richtigerweise müsste die Position der Datenschutzbehörden bei hypothetischer Zuständigkeit nicht die Abschaffung des Faxes sein, sondern die Forderung nach flächendeckendem Einsatz von SRTP. Sie könnten im Rahmen ihrer Zuständigkeit für die Landesbehörden auch entsprechend voran gehen. Stellungnahmen, die den Einsatz von SRTP als mögliche Lösung überhaupt erstmal ins Spiel bringen, wäre der Sicherheit dienlicher als Verbotsüberlegungen. Denn selbst, wenn man das Fax verbietet, besteht dasselbe Problem für Sprachtelefonie. Eigentlich müssten die Datenschutzbehörden mit ihrer Ansicht auch das Verbot des Telefons fordern (siehe kritisch auch Petrlic, DSB 2021, 88 ff.).

Fazit

Die Bremer Landesdatenschutzbeauftragte ist für die Beurteilung der Sicherheit von Faxen und Telefonie nicht zuständig. Unternehmen sollten sich davon nicht verunsichern lassen. BSI und BNetzA haben die Verschlüsselung bei VoIP zwar nur als „soll“-Vorschrift definiert, Datenschutzbeauftragte sollten gleichwohl für ihre Unternehmen darauf achten, dass künftig bei der Telekommunikation SRTP eingesetzt wird, um der Behauptung eines unsicheren Kommunikationsweges entgegen treten zu können.

Autor: **Jannik Krone ist Syndikusrechtsanwalt in Dresden und Rechtsanwalt bei Münch & Krone in Cottbus. Er ist dort schwerpunktmäßig im Datenschutz- und IT-Recht tätig.**