VERBAND DER INTERNETWIRTSCHAFT E.V.

STELLUNGNAHME

zu dem Vorschlag der Europäischen Kommission für eine Verordnung über Europäische Herausgabeanordnung und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM (2018) 225 final)

Berlin, 10.09.2018

eco – Verband der Internetwirtschaft nimmt die Gelegenheit wahr, zu dem Vorschlag der EU-Kommission zu elektronischen Beweismitteln in Strafsachen Stellung zu nehmen.

Grundsätzlich begrüßt eco den Vorschlag, ein einheitliches Verfahren für Herausgabe- und Sicherungsanordnungen für die gesamte Europäische Union zu etablieren. Dabei sollte allerdings grundsätzlich nicht aus dem Blick geraten, dass es sich hierbei zuallererst um die Wahrnehmung hoheitlicher Aufgaben handelt und die Verantwortung hierfür nicht auf Privatunternehmen abgewälzt werden darf. Zudem werfen weitere Punkte des Vorhabens aus Sicht der Internetwirtschaft Probleme auf.

I. Anordnungsbehörde (Artikel 4)

Nach Artikel 4 des Vorschlages der EU-Kommission ist vorgesehen, dass jede Justizbehörde (oder jede vom Anordnungsstaat bezeichnete zuständige Behörde in ihrer Eigenschaft als Ermittlungsbehörde) eines Mitgliedstaates befugt ist, eine Europäische Herausgabeanordnung oder Sicherungsanordnung zu erlassen und sich damit an die Diensteanbieter zu wenden, die ihre Dienste in der EU anbieten (Artikel 3).

Eine solche Lösung ist mit vielen Problemen und Unsicherheiten verbunden. Alleine in Deutschland gibt es 117 Staatsanwaltschaften, 638 Amtsgerichte und 115 Landgerichte. Dazu kommen noch diverse Fachgerichte. In den anderen Mitgliedstaaten sieht es ähnlich aus, im vergleichsweise viel kleineren Österreich beispielsweise gibt es über 20 (Ober)Staatsanwaltschaften, 114 Bezirks- und 18 Landesgerichte. Zudem ist die Justiz überall unterschiedlich organisiert. Für die Diensteanbieter ergibt sich so eine unübersehbare Anzahl an möglichen autorisierten Behörden und Personen.

Auch wenn Artikel 8 Absatz 2 vorsieht, dass die Übermittlung des Zertifikats über die Ermittlungs- oder Sicherungsanordnung (EPOC bzw. EPOC-PR) in einer Form erfolgen solle, die „einen schriftlichen Nachweis unter Bedingungen ermöglicht, die dem Adressaten die Feststellung der Echtheit gestatten“ ist keineswegs klar, wie diese Feststellung der Echtheit erfolgen soll. Denkbar wäre durchaus, dass der Diensteanbieter aufgrund der Fülle der autorisierten Behörden und der technischen Unklarheiten eine Manipulation gar nicht erkennen kann. Zudem bedeutete die jeweilige Prüfung im Einzelfall (Existenz der Behörde, Abgleich der Stempel o.ä.)

einen unangemessen hohen Aufwand, der durch eine andere Organisation der Arbeitsabläufe leicht vermieden werden könnte.

Das Problem ließe sich unter Umständen lösen, indem die EU-Kommission eine offizielle Liste der autorisierten Behörden herausgäbe, in der ausschließlich eine begrenzte Anzahl von Schwerpunktstellen benannt würden. Die einzelnen Länder könnten dann spezielle Justizbehörden qualifizieren oder einrichten, die sich mit der Validierung von Ermittlungs- und Sicherungsanordnungen befassen und diese an die Diensteanbieter weiterleiten. Ideal wäre hier natürlich eine Behörde pro Mitgliedstaat. Denkbar wäre aber auch eine Quotenregelung (z.B. eine Behörde pro ca. x Millionen Einwohner o.ä.). So ließe sich eine eventuelle Missbrauchsgefahr erheblich einschränken und der Aufwand für die Anbieter maßgeblich reduzieren.

Eine solche Vorgehensweise böte zudem weitere Vorteile: Zum einen dürften sich die Verfahren durch die Fachkenntnis der Behördenmitarbeiter abkürzen, es gäbe weniger Rückfragen wegen Unklarheiten, die Diensteanbieter hätten eine überschaubare Zahl fester Ansprechpartner, mit denen sich ein reibungsloser Arbeitsablauf viel besser gewährleisten ließe. Außerdem wäre es hier einfacher und rascher möglich, die technischen Voraussetzungen für eine sichere Übertragung der Daten zu schaffen. Realistischerweise muss nämlich davon ausgegangen werden, dass auch in einigen Jahren noch nicht jede Justizbehörde der Europäischen Union über absolut sichere Kommunikationskanäle verfügen wird.

II. Höchststrafenregelung (Artikel 5)

Voraussetzung für den Erlass einer EPOC oder EPOC-PR zur Herausgabe von Transaktions- und Inhaltsdaten soll nach Artikel 5 Absatz 4a des Vorschlags sein, dass die gegenständliche Straftat im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet wird. Diese Regelung bedürfte einer Einzelfallprüfung durch die Unternehmen; diese wäre schon deswegen notwendig, weil absolut unklar ist, ob ein Diensteanbieter haftet, wenn er Daten herausgibt, die Voraussetzungen für eine EPOC oder EPOC-PR aber nicht vorlagen. Eine derartige Einzelfallprüfung ist jedoch weder leistbar, noch sollte es Aufgabe der Anbieter sein, die Einschätzung staatlicher Stellen auf ihre Rechtmäßigkeit hin zu überprüfen.

Zudem ergäbe sich die unbefriedigende Situation, dass Diensteanbieter eines Mitgliedstaates möglicherweise Daten herausgeben müssten, obwohl die Tat in dem (Heimat-)Mitgliedstaat nicht strafbar oder weniger strafbewehrt ist. Ein Diensteanbieter sollte die Möglichkeit haben, sich in einem Land niederzulassen, in dem er die gesellschaftlichen Vorstellungen teilt und in dem er sich mit dem existierenden Recht identifizieren kann. Das könnte im Einzelfall untergraben werden, wenn ein Anbieter beispielsweise gezwungen wäre, Daten herauszugeben, damit ein Schwangerschaftsabbruch verfolgt werden kann.

Lösen ließen sich diese Probleme aus Sicht des eco durch eine verbindliche, einheitliche Liste der Europäischen Union, auf der – unabhängig von der Höhe der national teils unterschiedlichen Strafdrohung – konkrete Straftaten in einem Katalog verzeichnet sind, bei denen eine Herausgabe von Transaktions- und Inhaltsdaten gefordert werden kann. Durch eine genaue Beschreibung und Kommentierung dieses Katalogs sollte außerdem sichergestellt werden, dass die genannten Straftaten auch europaweit einheitlich ausgelegt werden.

Parallel dazu müssten die Strafprozessordnungen der Mitgliedstaaten angepasst werden: Insbesondere muss sichergestellt werden, dass Unternehmen keine Daten an ausländische Behörden herausgeben dürften, die im Inland mit einem Beweiserhebungs- oder verwertungsverbot belegt wären.

III. Haftung der Diensteanbieter

In diesem Zusammenhang ist nochmals darauf hinzuweisen, dass eine mögliche Haftung der Diensteanbieter im Vorschlag nicht geregelt ist. Um klarzustellen, dass die Anbieter nur auf staatliche Anordnung handeln bzw. nur durch den Staat angeordnete Maßnahmen ausführen, sollte im Gesetz ein Passus eingefügt werden, in dem eine Haftung der Unternehmen – außer bei Vorsatz und grober Fahrlässigkeit – ausgeschlossen wird. Dies sollte auch dann gelten, wenn eine Manipulation stattgefunden hat, dies dem Anbieter aber nicht ohne weiteres erkennbar war.

Diensteanbieter können keine Rechtsprüfung in 28 verschiedenen Rechtssystemen vornehmen; dies müssten sie aber, um eine mögliche Haftung sicher auszuschließen. Da eine Haftung der Diensteanbieter aber offenbar von der Kommission nicht intendiert ist, sollte dies ausdrücklich in die Verordnung aufgenommen und klargestellt werden: Es muss ganz deutlich werden, dass eine Rechtsprüfung ausschließlich durch Behörden erfolgt und diese etwaige Fehlentscheidungen auch zu vertreten haben.

Davon unabhängig muss klargestellt werden, dass ein Beweisverwertungsverbot für zu Unrecht erhobene bzw. herausgegebene Daten besteht. Des Weiteren muss ganz deutlich sein, dass es zu keiner Verwendung der Daten in Fällen außerhalb des ursprünglichen Grunds der Datenweitergabe kommen darf.

IV. Kostenerstattung

Zwar ist in Artikel 12 des Vorschlags grundsätzlich die Möglichkeit einer Kostenerstattung vorgesehen. Diese greift jedoch nur dann, wenn dies nach den „nationalen Rechtsvorschriften des Anordnungsstaats für innerstaatliche Anordnungen in ähnlichen Situationen vorgesehen ist“. Damit ist die Kostenerstattung uneinheitlich bzw. in einigen Staaten gar nicht vorhanden. Das ist sehr unbefriedigend, da es bürokratischen Aufwand verursacht, in 28 Mitgliedstaaten nach unterschiedlichen Vorschriften – wenn überhaupt –

Kosten abzurechnen. Zum anderen ist festzustellen, dass das Verfahren zur Herausgabe und Sicherung von Beweisen Hilfe zur staatlichen Aufgabenbewältigung darstellt und deswegen in jedem Fall angemessen auszugleichen ist.

Zu befürworten wäre daher eine EU-weit einheitliche Kostenregelung, speziell für die Herausgabe- und Sicherungsanordnung in der Verordnung.

V. Verhältnis zu Drittstaaten

Des Weiteren sollte im Gesetz klargestellt werden, dass kein Transfer der Daten in Drittstaaten erfolgen darf. Damit muss ausgeschlossen werden, dass einzelne Mitgliedstaaten eigene Abkommen mit Drittstaaten aushandeln, aufgrund derer bestimmte Daten dann weitergeleitet werden können. Ein solches Abkommen, das gegenseitige Verpflichtungen beinhaltet, sollte ausschließlich durch die gesamte Union begründet werden können.

Dazu wäre es in einem ersten Schritt wichtig, zu klären, wie der US-Cloud Act und der europäische Vorschlag zu elektronischen Beweismitteln zueinander stehen. Sodann sollte ein EU-US Übereinkommen ausgearbeitet werden, das beide Regelungen kompatibel macht.

VI. Verhältnis zur bestehenden Verfahren freiwilliger Kooperation

Klärungsbedürftig ist überdies die Frage, ob die mit E-Evidence beabsichtigten Befugnisse bzgl. ihres Regelungsgegenstandes abschließend zu verstehen sind. Dies ist deshalb von Bedeutung, weil die EPOC zumindest bzgl. bestimmten Herausgabemodalitäten (etwa bei der Herausgabe von Verkehrsdaten, die unter Richtervorbehalt stehen) strengere Vorgaben vorsieht als sie in bestehenden freiwilligen Kooperationsmodellen der Mitgliedstaaten auf Basis des geltenden Rechts greifen. Letztere spielen eine maßgebliche praktische Rolle für Herausgabeverlangen gegenüber Anbietern aus Nicht-EU-Staaten.

Für die betroffenen Anbieter muss klar sein, welche rechtsstaatlichen Standards gelten; aus Sicht des eco muss vermieden werden, dass für ein und dieselbe Herausgabekonstellation unterschiedliche Verfahren mit jeweils unterschiedlichen Standards gelten. Damit steht insgesamt die Frage im Raum, wie sich aus Sicht der Mitgliedsstaaten das Verhältnis zwischen EPCO und den heute bestehenden, überwiegend freiwilligen, Kooperationsmodellen darstellt.

VII. Harmonisierung der technischen Vorschriften

Ein weiterer wichtiger Punkt betrifft die Harmonisierung der technischen Vorschriften. Hierzu finden sich keine Vorgaben im Entwurf. In Deutschland dürfen sensible Daten beispielsweise nur verschlüsselt versendet werden. Eine Ausweitung dieser Regelung auf die Vorschriften zur Erlangung

elektronischer Beweismittel ist unverzichtbar, um die Sicherheit der Daten zu gewährleisten.

Zu empfehlen ist die Verschlüsselung und Verwendung einer einheitlichen ETSI-Schnittstelle, sowie die Verwendung einer technischen Schnittstelle, die die eindeutige Identifizierung von Absender und Adressat ermöglicht. Auch hier wird wieder deutlich, wie wichtig eine Begrenzung der Anzahl der zuständigen Behörden wäre.

Für eine harmonisierte technische Umsetzung der Anforderungen innerhalb der EU ist aus unserer Sicht der Erlass einer technischen Richtlinie begleitend zur Verordnung notwendig.

VIII. Keine Regelungen über Zeitfenster

Aus Sicht der Internetwirtschaft bedarf es außerdem keiner verbindlichen Regelungen über Zeitfenster. Der Zeitrahmen, der im Vorschlag der Kommission für die Ausführung von Herausgabe- und Sicherungsanordnungen vorgesehen ist, ist – insbesondere für KMU, die meistens keine 24/7-Dienste anbieten – nicht darstellbar. Das ist vor allem in Notfällen problematisch, für die ein Zeitfenster von sechs Stunden gelten soll. Dies stellt sehr viele Mitglieder des eco sowohl in den Abendstunden und der Nacht sowie an (langen) Wochenenden und Feiertagen vor unlösbare praktische Probleme. Bei derart kurzen Fristen bekommen sogar große Unternehmen Probleme, die ebenfalls kaum in der Lage sein dürften, zu jeder Tages- und Nachtzeit speziell geschultes Personal zur Verfügung zu halten.

Das Problem des Zeitablaufs ist vielmehr durch eine einfach und effizient organisierte Struktur zu lösen, in der eine oder wenige zuständige Behörden direkt mit zu benennenden Fachabteilungen der Unternehmen zusammenarbeiten.

Mindestens aber sollten für KMU Ausnahmeregelungen aufgenommen werden, um den Verwaltungsaufwand in Grenzen zu halten, der ihnen durch die Anforderungen entsteht. KMU würden ansonsten einen deutlichen Marktnachteil erleiden, was zu Problemen bei der Wettbewerbsfähigkeit führen würde, da nur größere Dienstleister in der Lage sein dürften, einen einseitigen Anstieg der Fix- und Grenzkosten abzufedern.

IX. Übergangs- und Umsetzungsfristen

Generell stellt die in Artikel 25 vorgesehene kurze Übergangsfrist von nur sechs Monaten eine unrealistische Annahme für die technische Umsetzung sowohl auf Seiten von Unternehmen als auch von Behörden dar. Als realistische Umsetzungsfristen dürften sich hier vielmehr 18 bis 24 Monate anbieten.

Über eco: *Mit über 1.000 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, formt Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Leitthemen sind Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie Ethik und Selbstregulierung. Deshalb setzt sich eco für ein freies, technikneutrales und leistungsstarkes Internet ein.*