EUROPÄISCHE ZENTRALBANK

EUROSYSTEM

DE **ECB-PUBLIC**

STELLUNGNAHME DER EUROPÄISCHEN ZENTRALBANK

vom 6. April 2017

zur Bestimmung Kritischer Infrastrukturen zum Zwecke der Sicherheit in der Informationstechnik

(CON/2017/10)

Einleitung und Rechtsgrundlage

Am 27. Februar 2017 wurde die Europäische Zentralbank (EZB) vom deutschen Bundesministerium des Innern um Stellungnahme zu einem ersten Verordnungsentwurf zur Änderung der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (nachfolgend der „Verordnungsentwurf") ersucht.

Die Zuständigkeit der EZB zur Abgabe einer Stellungnahme beruht auf Artikel 127 Absatz 4 und Artikel 282 Absatz 5 des Vertrags über die Arbeitsweise der Europäischen Union sowie auf Artikel 2 Absatz 1 fünfter Gedankenstrich der Entscheidung 98/415/EG des Rates[1], da der Verordnungsentwurf Zahlungs- und Verrechnungssysteme betrifft. Diese Stellungnahme wurde gemäß Artikel 17.5 Satz 1 der Geschäftsordnung der Europäischen Zentralbank vom EZB-Rat verabschiedet.

1. Ziel des Verordnungsentwurfs

1.1 Ziel des Verordnungsentwurfs ist die Bestimmung Kritischer Infrastrukturen und ihrer Betreiber, die dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (nachfolgend das „BSI-Gesetz") unterliegen, welches zuletzt durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme[2] geändert wurde. Das BSI-Gesetzenthält Pflichten dieser Betreiber, angemessene organisatorische und technische Vorkehrungen zum Schutz von infrastrukturbezogenen informationstechnischen Systemen (IT) zu treffen und erhebliche IT-Vorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Das BSI wird ermächtigt, Prüfungen vorzunehmen und die Durchführung von Maßnahmen zur Sicherstellung der Einhaltung des BSI-Gesetzes anzuordnen. Nach dem BSI-Gesetzhaben die Betreiber Kritischer Infrastrukturen das Recht auch die privilegierte Beratung und Information durch das BSI in Anspruch nehmen.

1.2 Durch die Festlegung zur Bestimmung von Infrastrukturen mit einer Schlüsselfunktion für verschiedene Bereiche der Gesellschaft zielt der Verordnungsentwurf darauf, Unsicherheiten dahingehend auszuräumen, welche Einrichtungen eine gegebene Kritische Infrastruktur betreiben.

---

1 Entscheidung 98/415/EG des Rates vom 29. Juni 1998 über die Anhörung der Europäischen Zentralbank durch die nationalen Behörden zu Entwürfen für Rechtsvorschriften (ABl. L 189 vom 3.7.1998, S. 42).

2 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17. Juli 2015.

1.3 In Bezug auf das Finanz- und Versicherungswesen umfasst der Verordnungsentwurf Folgendes: a) die Bargeldversorgung in den Bereichen Autorisierung einer Abhebung, Einbringen in den Zahlungsverkehr, Belastung Kundenkonto und Bargeldlogistik; b) den kartengestützten Zahlungsverkehr bei kartengebundenen Zahlungsvorgängen im Sinne der Verordnung (EU) Nr. 2015/751 des Europäischen Parlaments und des Rates[3] in den Bereichen Autorisierung und Einbringung in den Zahlungsverkehr sowie Belastung Kundenkonto und Gutschrift auf dem Konto des Zahlungsempfängers; c) den konventionellen Zahlungsverkehr mittels Überweisung und Lastschrift im Sinne der Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates[4] in den Bereichen Annahme einer Überweisung oder Lastschrift, Einbringen in den Zahlungsverkehr sowie Belastung und Gutschrift Kundenkonto; d) die Verrechnung und die Abwicklung von Wertpapier- und Derivatgeschäften, einschließlich Verbuchung Wertpapiere und Verbuchung Geld sowie e) Versicherungsdienstleistungen.

1.4 Sowohl mit dem BSI-Gesetz als auch mit dem Verordnungsentwurf wird die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates[5] umgesetzt, zu der die EZB eine Stellungnahme veröffentlicht hat[6]. Mit dem Verordnungsentwurf wird Artikel 5 Absatz 1 und Anhang II der Richtlinie (EU) 2016/1148 umgesetzt, welche gemeinsam den Anwendungsbereich der Richtlinie festlegen.

1.5 Über die Erfordernisse der Richtlinie (EU) 2016/1148 hinaus führt die Begründung zum Verordnungsentwurf explizit TARGET2, SWIFT, EURO1, STEP1 und STEP2-T als Beispiele für Infrastrukturen auf, die dem BSI-Gesetz unterliegen. Insbesondere werden diese Systeme als „System zur Anbindung an ein Interbanken-Zahlungsverkehrssystem“ eingestuft, die den Kategorien „Infrastrukturen zur Bargeldversorgung“ und „konventioneller Zahlungsverkehr“ im Teil 1 Nummer 1 des Anhangs 6 des Verordnungsentwurfs zugeordnet sind.

1.6 Vom Geltungsbereich werden durch das BSI-Gesetz Betreiber Kritischer Infrastrukturen ausgenommen, soweit sie auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen des BSI-Gesetzes vergleichbar oder weitergehend sind[7].

2. Allgemeine Anmerkungen

2.1 Wie bereits erwähnt[8], befürwortet die EZB das Ziel der Richtlinie (EU) 2016/1148, eine hohe gemeinsame Netz- und Informationssicherheit in der Union zu gewährleisten und in diesem Bereich in allen Unternehmenssektoren und Mitgliedstaaten einen einheitlichen Ansatz zu verwirklichen. Dabei ist es wichtig sicherzustellen, dass der Binnenmarkt ein sicherer

---

3 Verordnung (EU) Nr. 2015/751 des Europäischen Parlaments und des Rates vom 29. April 2015 über Interbankenentgelte für kartengebundene Zahlungsvorgänge (ABl. L 123 vom 19.5.2015, S. 1).

4 Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro (ABl. L 94 vom 30.3.2012, S. 22)..

5 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

6 Siehe Stellungnahme CON/2014/58. Alle Stellungnahmen der EZB werden auf der Website der EZB unter www.ecb.europa.eu veröffentlicht.

7 §§ 8c Absatz 2 Nummer 4 und 8c Absatz 3 Nummer 4 des BSI-Gesetzes.

8 Siehe Nummer 2.1 der Stellungnahme CON/2014/58.

Wirtschaftsstandort ist und dass alle Mitgliedstaaten für den Fall von Netzsicherheitsvorfällen über ein bestimmtes Mindestniveau an Abwehrbereitschaft verfügen.

2.2 Auch wenn der Verordnungsentwurf auf die Stärkung der allgemeinen Widerstandsfähigkeit Kritischer Infrastrukturen durch die Bestimmung von Infrastrukturen mit einer Schlüsselfunktion für verschiedene Bereiche der Gesellschaft zielt, sollte sichergestellt werden, dass die Rechtsvorschriften des Verordnungsentwurfs nicht in den Zuständigkeitsbereich des Eurosystems eingreifen. Dies könnte durch die ausdrückliche Ausnahme aus dem Geltungsbereich der durch die EZB und das Eurosystem im Allgemeinen, einschließlich der durch die Deutsche Bundesbank überwachten und/oder betriebenen Zahlungs- und Verrechnungssysteme aus erfolgen, da diese vergleichbaren oder strengeren Anforderungen unterliegen. Im Wesentlichen muss gewährleistet sein, dass die Umsetzung der Anforderungen der Richtlinie (EU) 2016/1148 nicht mit der Verordnung (EU) Nr. 795/2014 der Europäischen Zentralbank (EZB/2014/28)[9] und dem Rahmen der Überwachungspolitik des Eurosystems kollidiert. Eine Erweiterung des Geltungsbereichs des BSI-Gesetzes auf die durch die EZB und das Eurosystem im Allgemeinen, einschließlich der durch die Deutsche Bundesbank betriebenen und/oder überwachten Infrastrukturen würde Anlass zu erheblichen Bedenken im Hinblick auf den Grundsatz des Vorrangs des Unionsrechts sowie im Hinblick auf den Grundsatz der Unabhängigkeit der Zentralbanken gemäß Artikel 130 des Vertrags geben.

2.3 Ungeachtet der vorstehenden Ausführungen ist die EZB bereit, mit dem BSI zusammenzuarbeiten, um sicherzustellen, dass bewährte Vorgehensweisen und Standards für die Netz- und Informationssicherheit geschaffen und befolgt werden.

2.4 Schließlich scheint eine ausreichende Rechtsgrundlage im Verordnungsentwurf selbst zu fehlen, damit die durch die EZB und das Eurosystem, einschließlich der durch die Deutsche Bundesbank betriebenen und überwachten Infrastrukturen dem BSI-Gesetz unterliegen. Entgegen der beabsichtigten Anwendung des BSI-Gesetzes auf die durch das Eurosystem betriebenen Infrastrukturen bestehen Zweifel, ob die Definition der Kritischen Infrastrukturen im Sinne des § 2 Absatz 10 des BSI-Gesetzes diese Infrastrukturen abdeckt. Zwar verweist diese Bestimmung generell auf das „Finanz- und Versicherungswesen“, die Begründung zum Entwurf des BSI-Gesetzes legt jedoch in einer abschließenden Liste die für diesen Bereich relevanten Teilsektoren fest, die eine Grundlage für die für das Bankwesen, die Finanzdienstleister, Wertpapierbörsen und Versicherungsgesellschaften geltenden Vorschriften des abgeleiteten Rechts bilden sollten. Zentralbanken werden in dieser Liste nicht aufgeführt. Gemäß dem vom Gerichtshof der Europäischen Union festgelegten Grundsatz, dass Bestimmungen des nationalen Rechts im Einklang mit der umzusetzenden Richtlinie auszulegen sind[10], ist anzumerken, dass Anhang II der Richtlinie (EU) 2016/1148 Zentralbanken nicht als Betreiber wesentlicher Dienstleistungen aufführt. Zentralbanken sind keine Kreditinstitute im Sinne der Definition „Bankwesen“, da Kreditinstitute unter Bezugnahme auf Artikel 4 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 575/2013 des

---

9 Verordnung (EU) Nr. 795/2014 der Europäischen Zentralbank vom 3. Juli 2014 zu den Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme (EZB/2014/28) (ABl. L 217 vom 23.7.2014, S. 16).

10 *Amministrazione delle Finanze dello Stato gegen Simmenthal SpA*., C-106/77, ECLI:EU:C:1978:49; *Marleasing SA gegen La Comercial Internacional de Alimentacion SA.*, C-106/89, ECLI:EU:C:1990:395.

Europäischen Parlaments und des Rates[11] definiert werden. Die Verordnung (EU) Nr. 575/2013 legt einheitliche Vorschriften in Bezug auf die allgemeinen Aufsichtsanforderungen fest, die unter die Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates[12] fallende Kreditinstitute und Wertpapierfirmen erfüllen müssen. Zentralbanken sind vom Geltungsbereich der Richtlinie 2013/36/EU ausgenommen und sind somit keine dem Geltungsbereich der Verordnung (EU) Nr. 575/2013 unterstehenden beaufsichtigten Institute. Daher unterstehen weder die EZB noch die Deutsche Bundesbank dem Geltungsbereich des Bankwesens gemäß Nummer 3 des Anhangs II der Richtlinie (EU) 2016/1148.

2.5 Die EZB und die Bundesbank unterstehen nicht dem Geltungsbereich von „Finanzmarktinfrastrukturen" im Sinne der Nummer 4 des Anhangs II der Richtlinie (EU) 2016/1148, da sie keine Handelsplätze im Sinne des Artikels 4 Nummer 24 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates[13] betreiben, die vom Geltungsbereich dieser Richtlinie gemäß Artikel 2 Absatz 1 Buchstabe h ausgenommen sind. Die Mitglieder des Europäischen Systems der Zentralbanken (ESZB) sind keine zentralen Gegenparteien im Sinne des Artikels 2 Absatz 1 der Verordnung (EU) Nr. 648/2012[14], da Mitglieder des ESZB vom Geltungsbereich dieser Verordnung gemäß Artikel 1 Absatz 4 Buchstabe a ausgenommen werden.

3. Auswirkung des Verordnungsentwurfs auf die durch die EZB und das Eurosystem überwachten Zahlungssysteme

3.1 Die EZB nimmt insbesondere zur Kenntnis, dass die Begründung zum Verordnungsentwurf explizit TARGET2, EURO1 und STEP2-T als Beispiele für Infrastrukturen aufführt, die dem BSI-Gesetz unterliegen sollen.[15] Diese Zahlungssysteme wurden gemäß des Beschlusses EZB/2014/35 der Europäischen Zentralbank[16] bzw. des Beschlusses EZB/201436 der Europäischen Zentralbank[17] als systemrelevante Zahlungsverkehrssysteme (systemically important payment systems – SIPS) identifiziert und die EZB ist die zuständige Behörde gemäß der Verordnung (EU) Nr. 795/2014 (EZB/2014/28) zu ihrer Überwachung. Bei den aufgeführten SIPS spielt vor allem TARGET2 eine

---

11 Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 176 vom 27.6.2013, S. 1).

12 Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).

13 Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. L 173 vom 12.6.2014, S. 349).

14 Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister (ABl. L 201 vom 27.7.2012, S. 1).

15 STEP1, was nach dem Verordnungsentwurf auch als Kritische Infrastruktur identifiziert wird, ist primär ein Zahlungsdienst für den Geschäftsverkehr und ist für die Bearbeitung einzelner grenzüberschreitender Zahlungen in Euro konzipiert. STEP1 profitiert dabei von der technischen und rechtlichen Infrastruktur des EURO1; Teilnehmer an den STEP1-Dienstleistungen können vollständig die EURO1-Plattform nutzen und sind direkt mit sämtlichen EURO1- und STEP1-Teilnehmern verbunden.

16 Beschluss EZB/2014/35 der Europäischen Zentralbank vom 13. August 2014 zur Bestimmung von TARGET2 als ein systemrelevantes Zahlungsverkehrssystem gemäß der Verordnung (EU) Nr. 795/2014 zu den Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme (ABl. L 245 vom 20.8.2014, S. 5).

17 Beschluss EZB/2014/36 der Europäischen Zentralbank vom 13. August 2014 zur Bestimmung von EURO1 und STEP2-T als systemrelevante Zahlungsverkehrssysteme gemäß der Verordnung (EU) Nr. 795/2014 zu den Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme.

bedeutende Rolle, da es im Eigentum und im Betrieb des Eurosystems steht und einer strengen Regulierung und Überwachung untersteht.

3.2 Der Verordnungsentwurf stuft TARGET2, EURO1 und STEP2-T fälschlicherweise als Beispiele für „Systeme zur Anbindung an Interbanken-Zahlungsverkehrssysteme“ ein. Sie sollten allerdings vielmehr als Zahlungssysteme zur Tätigung des konventionellen Zahlungsverkehrs eingestuft werden. Aufgrund des Verweises in § 7 Absatz 4 des Verordnungsentwurfs auf die Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates[18], die Bestimmungen zu Massenzahlungssystemen enthält, sind bei konventionellen Zahlungsvorgängen sämtliche Zahlungen, die auf einem Großbetragszahlungssystem wie TARGET2 und EURO1 ausgeführt werden, vom Geltungsbereich des konventionellen Zahlungsverkehrs ausgenommen.

3.3 Gemäß Artikel 127 Absatz 2 vierter Gedankenstrich des Vertrags ist die Förderung des reibungslosen Funktionierens der Zahlungssysteme eine der Kernaufgaben des ESZB. Darüber hinaus können die EZB und die nationalen Zentralbanken gemäß Artikel 22 der Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank (nachfolgend die „Satzung des ESZB“) Einrichtungen zur Verfügung stellen und die EZB kann Verordnungen erlassen, um effiziente und zuverlässige Verrechnungs- und Zahlungssysteme innerhalb der Union zu gewährleisten. Dementsprechend haben die EZB und das Eurosystem insgesamt ein besonderes Interesse an einer verbesserten Netz- und Informationssicherheit in Bezug auf Zahlungssysteme, da es das Vertrauen in den Euro und das reibungsloses Funktionieren der Wirtschaft in der Union stärkt.

3.4 Innerhalb des Euro-Währungsgebiets unterliegen SIPS den Anforderungen der Verordnung (EU) Nr. 795/2014 (EZB/2014/28). Mit dieser Verordnung werden die Prinzipien für Finanzmarktinfrastrukturen des Ausschusses für Zahlungsverkehr und Marktinfrastrukturen (Committee on Payments and Market Infrastructures – CPMI) und des Ausschusses der Internationalen Organisation der Wertpapieraufsichtsbehörden (International Organization of Securities Commissions − IOSCO) (nachfolgend die „CPMI-IOSCO-Prinzipien“)[19] in rechtlich bindender Weise umgesetzt und Großbetrags- und Massenzahlungssysteme von systemischer Bedeutung, die entweder von einer Zentralbank des Eurosystems oder von einem privaten Unternehmen betrieben werden, umfasst. Demnach unterliegen SIPS einer regelmäßigen Beurteilung hinsichtlich der Anforderungen der Verordnung (EU) Nr. 795/2014 (EZB/2014/28) in Bezug auf das operationelle Risiko und die entsprechend zuständige Behörde darf überprüfen, ob die Systeme diesen Anforderungen entsprechen. Im Fall der Nichteinhaltung hat die zuständige Behörde die Befugnis, Sanktionen oder Korrekturmaßnahmen zur Sicherstellung der Einhaltung aufzuerlegen.

3.5 Im Einklang mit der Empfehlung der EZB[20] bleiben gemäß Erwägungsgrund 14 der Richtlinie (EU) 2016/1148 die bestehenden unionsrechtlichen Bestimmungen zur Überwachung von

---

18 Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro und zur Änderung der Verordnung (EG) Nr. 924/2009 (ABl. L 94 vom 30.3.2012, S. 22).

19 Verfügbar auf der Website der Bank für Internationalen Zahlungsausgleich unter www.bis.org .

20 Siehe Nummer 3.1 der Stellungnahme CON/2014/58.

Zahlungsverkehrs- und Abwicklungssystemen durch das Eurosystem unberührt. Zwar wird in Artikel 3 der Richtlinie klargestellt, dass die Richtlinie nur die Maßnahmen zur Mindestharmonisierung festlegt und die Mitgliedstaaten Bestimmungen erlassen oder aufrechterhalten können, mit denen ein höheres Sicherheitsniveau von Netz- und Informationssystemen erreicht werden soll, allerdings wird auch gesagt, dass dies die Verpflichtungen der Mitgliedstaaten nach dem Unionsrecht unberührt lässt. In diesem Zusammenhang ist es wichtig zu betonen, dass bereits anwendbare wirksame Vorschriften für die Sicherheit von SIPS im Rechtsrahmen der Union zur Überwachung der Zahlungssysteme bestehen. Genauer gesagt werden durch die Verordnung (EU) Nr. 795/2014 (EZB/2014/28) eine Reihe von rechtlichen Anforderungen an SIPS gestellt, die auch das operationelle Risiko betreffen, einschließlich der Verpflichtung a) umfassende Richtlinien für die physische Sicherheit und die Informationssicherheit zur angemessenen Erkennung, Bewertung und Begegnung aller möglichen Schwachstellen und Bedrohungen festzulegen, und b) bei kritischen informationstechnischen Systemen sicherzustellen, dass sie ihren Betrieb innerhalb näher bestimmter Fristen im Fall eines Ereignisses, das mit einer erheblichen Gefahr einer Störung der Geschäfte des SIPS verbunden ist, wieder aufnehmen können.[21] Schließlich wird in Erwägungsgrund 13 der Richtlinie (EU) 2016/1148 anerkannt, dass die Anforderungen an das operationelle Risiko bei Finanzmarktinfrastrukturen (wie z. B. SIPS) aus Rechtsakten der Union oftmals die in der Richtlinie festgelegten Anforderungen übertreffen und dementsprechend als *Lex Specialis* anzusehen sind und den nationalen Regelungen zur Umsetzung der Richtlinie (EU) 2016/1148 vorgehen.

3.6 Es gibt Pläne den bestehenden Rechtsrahmen der Union zur Überwachung von Zahlungssystemen zu verbessern. Insbesondere die Verordnung (EU) Nr. 795/2014 (EZB/2014/28) befindet sich derzeit in einer allgemeinen Überprüfung ihrer Anwendung und zu einem überarbeiteten Entwurf der Verordnung (EU) Nr. 795/2014 (EZB/2014/28) wurde ein öffentliches Konsultationsverfahren im Dezember 2016[22] durchgeführt. Der Verordnungsvorschlag zur Änderung der Verordnung (EU) Nr. 795/2014 (EZB/2014/28) ist auf eine weitere Stärkung der Anforderungen zum operationellen Risiko und zur Netz- und Informationssicherheit ausgelegt und berücksichtigt unter anderem die CPMI-IOSCO-Prinzipien für Finanzmarktinfrastrukturen zur Widerstandsfähigkeit gegenüber Cyberangriffen.[23] Es werden eine Reihe neuer Anforderungen eingeführt, mit denen operationellen und Cyberrisiken begegnet werden soll und mit denen SIPS-Betreiber verpflichtet werden, folgende Schritte zu unternehmen: a) die Überprüfung, Untersuchung und Prüfung der Systeme, betrieblichen Vorgaben, Verfahren und Kontrollen in regelmäßigen Abständen und nach erheblichen Änderungen am System; b) die Errichtung eines wirksamen Rahmens zur Widerstandsfähigkeit gegenüber Cyberangriffen und dazu das Vorhalten geeigneter Steuerungsmaßnahmen für das Cyberrisikomanagement; c) die Ermittlung ihrer kritischen Geschäfte und unterstützenden Vermögenswerte und das Vorhalten geeigneter Maßnahmen zum Schutz vor, zur Aufdeckung von, zur Reaktion auf und zur Erholung von Cyberangriffen; d) die Testung der eingeführten Maßnahmen und e) das Verfügen über ein solides

21 Siehe Artikel 15 der Verordnung (EU) Nr. 795/2014 (EZB/2014/28).

22 Abrufbar auf der Website der EZB unter www.ecb.europa.eu.

23 Auf der Website der Bank für Internationalen Zahlungsausgleich unter http://www.bis.org.

Maß an Situationsbewusstsein für Cyberbedrohungen, einschließlich eines Verfahrens zum kontinuierlichen Lernen[24]. Die vorgeschlagenen neuen Regelungen sind ebenso als sektorspezifische Unionsgesetzgebung einzustufen, die zumindest eine ähnliche Auswirkung im Sinne des Artikels 1 Absatz 7 der Richtlinie (EU) 2016/1148 haben und dementsprechend nationalen Regelungen zur Umsetzung der Richtlinie vorgehen sollte. Im Ergebnis könnten die vorstehend genannten SIPS vom Geltungsbereich des Verordnungsentwurfs ausgenommen sein.

3.7 Im Einklang mit den in der Richtlinie (EU) 2016/1148[25]festgelegten Anforderungen ist in Verordnung (EU) Nr. 795/2014 (EZB/2014/28) die Befugnis der zuständigen Behörden vorgesehen, Informationen zu unter anderen schwerwiegenden und gerinfügigeren Vorfällen, zu Art und Charakter des Vorfalls, ihrer Schwere und ihrer Dauer zu erhalten[26]. Zugleich werden mit dem Verordnungsvorschlag zur Änderung der Verordnung (EU) Nr. 795/2014 (EZB/2014/28) die Befugnisse der zuständigen Behörden, Vor-Ort-Prüfungen durchzuführen und Untersuchungen oder unabhängige Überprüfungen der Funktionsfähigkeit des Systems zu verlangen, weiter verbessert[27].

3.8 Ähnlich wie SIPS, die der Verordnung (EU) Nr. 795/2014 (EZB/2014/28) unterliegen, unterliegen die zwei anderen Kategorien der Nicht-SIPS, das sind besonders bedeutsame Massenzahlungssysteme (prominently important retail payment systems – PIRPS) und andere Massenzahlungssysteme (other retail payment systems – ORPS), vergleichbaren Überwachungsstandards. Dem überarbeiteten Überwachungsrahmen für Massenzahlungsverkehrssysteme des Eurosystems[28] zufolge unterliegen sowohl PIRPS und ORPS den CPMI-IOSCO-Prinzipien, insbesondere dem Prinzip 17 zum operationellen Risiko[29].

3.9 Zwar ist das Ziel des Verordnungsentwurfs Artikel 5 Absatz 1 der Richtlinie (EU) 2016/1148 umzusetzen, indem die Betreiber grundlegender Dienstleistungen mit einer Niederlassung auf dem Staatsgebiet von Deutschland ermittelt werden, allerdings ist fraglich, ob die ermittelten Zahlungssysteme als „effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung“ in Deutschland angesehen werden können[30]. Obwohl anerkannt wird, dass die Kritischen Infrastrukturen deutschem Recht unterliegen, sollte das zugrundeliegende Recht nicht als entscheidender Faktor für die Beurteilung ihre Kritikalität in Bezug auf das deutsche Hoheitsgebiet herangezogen werden, da sich in vielen Fällen die physische Infrastruktur zu einem gewissen Grad auch außerhalb des deutschen Hoheitsgebiets befindet[31].

---

24 Siehe Artikel 1 Absatz 9 Buchstaben a und b des Verordnungsvorschlags zur Änderung der Verordnung (EU) Nr. 795/2014 (EZB/2014/28).

25 Siehe Artikel 14 Absatz 3.

26 Siehe Artikel 21 der Verordnung (EU) Nr. 795/2014 (EZB/2014/28).

27 Siehe Artikel 1 Absatz 12 Buchstaben b und c des Verordnungsvorschlags zur Änderung der Verordnung (EU) Nr. 795/2014 (EZB/2014/28).

28 Abrufbar auf der Website der EZB unter www.ecb.europa.eu.

29 Dies beinhaltet die wesentlichen Erwägungen 1, 3 und 5 des Prinzips 17.

30 Siehe Erwägungsgrund 21 der Richtlinie (EU) 2016/1148.

31 Im Hinblick auf TARGET2 trifft dies nur für die Teilkomponenten TARGET2-EZB und TARGET2-Deutsche Bundesbank zu. Es wird auch darauf hingewiesen, dass EURO1 und STEP2-T durch einen Rechtsträger mit Sitz in Frankreich betrieben werden.

4. Auswirkung des Verordnungsentwurfs auf TARGET2-Securities

4.1 In Anbetracht der abstrakten Kriterien des Verordnungsentwurfs, auf die in Nummer 1.3 Bezug genommen wird, geht die EZB davon aus, dass auch TARGET2-Securities (T2S) in den Geltungsbereich des Verordnungsentwurfs fallen könnten.

4.2 T2S ist ein vom Eurosystem eingerichteter Dienst für die Wertpapierabwicklung in Zentralbankgeld, der Zentralverwahrern (central securities depositories – CSD) als Bestandteil der Aufgaben des Eurosystems gemäß den Artikeln 17, 18 und 22 der ESZB-Satzung zur Verfügung gestellt werden soll. T2S basiert auf einer einzigen technischen Plattform, die in die Echtzeit-Brutto-Zahlungsverkehrssysteme der Zentralbanken integriert ist.[32] T2S ist systemrelevant, da es kritische grundlegende Abwicklungsdienste für die CSD zur Verfügung stellt.

4.3 Im Einklang mit dem Beschluss des EZB-Rats in seinem Rahmen der Überwachungspolitik des Eurosystems vom Juli 2011 fällt T2S in die Zuständigkeiten des Eurosystems zur Überwachung gemäß Artikel 127 Absatz 2 des Vertrages sowie Artikel 3 Absatz 1 und Artikel 22 der ESZB-Satzung[33]. Diese Zuständigkeiten werden im Einklang mit den CPMI-IOSCO-Prinzipien ausgeübt. Die Überwachungsfunktion des Eurosystems über T2S wird in vergleichbarer Weise in der T2S-Rahmenvereinbarung anerkannt, dem zentralen T2S-Vertragsdokument, das die Regeln für die Erbringung von T2S-Dienstleistungen durch das Eurosystem für CSD festlegt[34]. Darüber hinaus arbeitet das Eurosystem im Rahmen der Überwachung von T2S mit den für die Überwachung und Beaufsichtigung von dem T2S angeschlossenen CSD zuständigen nationalen Behörden auf der Grundlage eines Memorandums of Understanding zwischen der EZB und diesen Behörden zusammen. Das T2S als vom Geltungsbereich des Verordnungsentwurfs erfasst zu betrachten, würde in die Zuständigkeiten des Eurosystems, die sich aus dem Vertrag ergeben, eingreifen. Der Verordnungsentwurf sollte daher geändert werden, um T2S eindeutig aus dem Geltungsbereich auszunehmen.

5. Auswirkung des Verordnungsentwurfs auf die vom Eurosystem überwachten Zahlungssysteme

5.1 Kartengestützter Zahlungsverkehr und konventionelle Zahlungsvorgänge sollten nicht dem Geltungsbereich des Verordnungsentwurfs unterstehen, da dies in die bestehenden Aufsichts- und Überwachungszuständigkeiten des Eurosystems eingreifen würde.

5.2 Zwar könnten Infrastrukturen im Zusammenhang mit kartengestütztem Zahlungsverkehr und konventionellen Zahlungsvorgängen, z. B. Überweisungen und Lastschriften, dem Geltungsbereich des Verordnungsentwurfs unterstehen, doch ist dazu anzumerken, dass Zahlungsinstrumente wie Karten, Überweisungen, Lastschriften und E-Geld im Rahmen der Überwachungspolitik des Eurosystems als ein „integraler Bestandteil des Zahlungssystems“ bezeichnet werden und sie damit zum Geltungsbereich seiner Zentralbanküberwachung zählen. Für Zahlungsinstrumente erfolgt die Zuweisung der Rolle der hauptverantwortlichen Aufsichtsinstanz (für das Eurosystem) durch Bezugnahme auf die nationale Verankerung des Zahlungssystems und die rechtliche

32 Siehe Artikel 1 Absatz 1 der Leitlinie EZB/2012/13.

33 Siehe Abschnitt 4.4 der überarbeiteten Fassung des Rahmens der Überwachungspolitik des Eurosystems „Eurosystem Oversight Policy Framework“ (Juli 2016), abrufbar auf der Website der EZB unter www.ecb.europa.eu.

34 Siehe Artikel 18.

Verankerung seiner „Governance Authority“. Für Überweisungs- und Lastschriftsysteme im einheitlichen Euro-Zahlungsverkehrsraum sowie für einige der internationalen Kartenzahlungssysteme hat die EZB die federführende Aufsichtsfunktion inne.

5.3 Während Zahlungsdienstleister, die Zahlungsdienstleistungen über Zahlungsinstrumente erbringen, von den zuständigen Behörden beaufsichtigt werden, erfolgt die Überwachung der zugrundeliegenden kritischen Finanzmarktinfrastrukturen durch das Eurosystem. Zur Gewährleistung einer hohen Netz- und Informationssicherheit unterliegen Zahlungsdienstleister der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates[35], die ab Januar 2018 anwendbar ist. Die Richtlinie legt strenge Leitlinien zur Meldung von schwerwiegenden Vorfällen (in Artikel 96), zu Sicherheitsmaßnahmen für operationelle und sicherheitsrelevante Risiken (in Artikel 95) und zu technischen Regulierungsstandards für eine starke Kundenauthentifizierung und sichere Kommunikation (in Artikel 98) fest. Diese Leitlinien wurden von der Europäischen Bankenaufsichtsbehörde in Zusammenarbeit mit der EZB erstellt.

6. Auswirkung des Verordnungsentwurfs auf kritische Dienstleister

6.1 Entgegen der Begründung zum Verordnungsentwurf, in der explizit die Society for Worldwide Interbank Financial Telecommunication (SWIFT) als dem BSI-Gesetz unterliegende Infrastruktur aufgeführt wird, sollte SWIFT vom Geltungsbereich des Verordnungsentwurfs ausgenommen werden. SWIFT stellt sichere Nachrichtendienstleistungen in einer großen Zahl von Ländern zur Verfügung und ist eine genossenschaftliche Gesellschaft mit beschränkter Haftung mit Sitz in Belgien, deren Infrastrukturknoten sich nicht auf deutschem Hoheitsgebiet befinden. Die Nationale Bank van België / Banque Nationale de Belgique ist die oberste Überwachungsbehörde von SWIFT und führt auf der Grundlage einer kooperativen Überwachung in Zusammenarbeit mit den anderen G10-Zentralbanken, einschließlich der EZB und der Deutschen Bundesbank, die Überwachung von SWIFT durch.

6.2 Die G10-Überwachungsorgane erkennen an, dass der Hauptschwerpunkt der Überwachung auf dem operationellen Risiko von SWIFT liegt, da dieses als die wichtigste Risikokategorie betrachtet wird, durch die SWIFT ein Systemrisiko für das Finanzsystem in der Union darstellen könnte. Die kooperative Überwachungsgruppe von SWIFT hat diesbezüglich ein spezifisches Bündel von Grundsätzen und einen Erwartungskatalog („High Level Expectations“) entwickelt, die auf SWIFT Anwendung finden, wie zum Beispiel Risikoidentifizierung und -management, Informationssicherheit, Zuverlässigkeit und Widerstandsfähigkeit, Technologieplanung und Kommunikation mit Anwendern. Die G10-Überwachungsorgane unterziehen SWIFT einer intensiven Form der Überwachung und erwarten, dass SWIFT insbesondere die CPMI-IOSCO-Prinzipien zur Widerstandsfähigkeit gegenüber Cyberangriffen und andere internationale IT-Sicherheitsstandards einhält, die über die in der Richtlinie (EU) 2016/1148 festgelegten Anforderungen hinausgehen.

35 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35).

7. Auswirkung des Verordnungsentwurfs auf andere Finanzmarktinfrastrukturarten

7.1 Während zentrale Gegenparteien (Central Clearing Counterparties, CCP) und CSD in den Anwendungsbereich des Verordnungsentwurfs fallen können, ist anzumerken, dass solche Finanzmarktstrukturen gemäß der Verordnung (EU) Nr. 648/2012 und der Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates[36], in denen Anforderungen zum operationellen Risiko festgelegt sind, bereits von verschiedenen Behörden streng reguliert und überwacht werden. Darüber hinaus sollten beide Arten von Finanzmarktinfrastrukturen die CPMI-IOSCO-Netzsicherheitsempfehlungen zur Kenntnis nehmen, die für alle Finanzmarktinfrastrukturen gelten.

7.2 Neben den an die nationalen zuständigen Behörden gemäß der Verordnung (EU) Nr. 648/2012 und der Verordnung (EU) Nr. 909/2014 übertragenen Aufsichtszuständigkeiten ist anzumerken, dass den nationalen Behörden, insbesondere den Mitgliedern des ESZB, Zuständigkeiten zur Überwachung in Bezug auf diese Finanzmarktinfrastrukturen übertragen werden können. In Erwägungsgrund 11 der Verordnung (EU) 648/2012 wird diesbezüglich klargestellt, dass eine der grundlegenden Aufgaben des Europäischen Systems der Zentralbanken (ESZB) darin besteht, das reibungslose Funktionieren der Zahlungssysteme zu fördern. In diesem Zusammenhang führen die Mitglieder des ESZB die Überwachung durch, indem sie für effiziente und solide Clearing- und Zahlungssysteme einschließlich CCP sorgen. Des Weiteren wird durch die Verordnung (EU) Nr. 648/2012 die Zuständigkeit der EZB und der NZBen für die Gewährleistung effizienter und solider Clearing- und Zahlungssysteme innerhalb der Europäischen Union und im Verhältnis zu anderen Ländern nicht berührt.

7.3 Ebenso hält Erwägungsgrund 8 der Verordnung (EU) Nr. 909/2014 in Bezug auf CSD fest, dass die Verordnung die Zuständigkeit der EZB und der NZBen für die Gewährleistung effizienter und solider Clearing- und Zahlungssysteme innerhalb der Europäischen Union und im Verhältnis zu anderen Ländern nicht berühren sollte und dem Zugang der Mitglieder des ESZB zu den Informationen, die für die Erfüllung ihrer Aufgaben, einschließlich der Überwachung von Zentralverwahrern und anderen Finanzmarktinfrastrukturen, zweckdienlich sind, nicht entgegenstehen sollte.

7.4 Die EZB ist daher der Auffassung, dass die potenzielle Einbeziehung von CCP und CSD in den Geltungsbereich des Verordnungsentwurfs in die bestehenden Aufsichts- und Überwachungszuständigkeiten eingreifen könnte. Der Verordnungsentwurf sollte daher geändert werden, um a) klarzustellen, dass die Zuständigkeiten des BSI gemäß dem Verordnungsentwurf die Aufgaben der zuständigen Behörden, einschließlich der für die Überwachung und Beaufsichtigung der CCP und CSD verantwortlichen Mitglieder des ESZB nicht berühren bzw. diesen angepasst werden, und b) die Anwendung sämtlicher sich aus dem Verordnungsentwurf ergebenden Anforderungen auf diese Finanzmarktinfrastrukturen zu vermeiden, bei denen es zu

36 Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Europäischen Union und über Zentralverwahrer sowie zur Änderung der Richtlinien 98/26/EG und 2014/65/EU und der Verordnung (EU) Nr. 236/2012 (ABl. L 257 vom 28.8.2014, S. 1).

Überlappungen mit den auf CCP und CSD anwendbaren *Lex Specialis*-Anforderungen gemäß ihrem jeweiligen Aufsichts- und Überwachungsrahmen kommen könnte.

Diese Stellungnahme wird auf der Website der EZB veröffentlicht.

Geschehen zu Frankfurt am Main am 6. April 2017.

[*Unterschrift*]

Der Präsident der EZB

Mario DRAGHI