www.jusletter-it.eu

Helgo Eberwein / Árpád Geréd

Bits Coins

Herausforderungen für sichere Zahlungsdienste im 21. Jahrhundert

Die derzeit bedeutendste virtuelle Währung Bitcoin wird im Hinblick auf die kapitalmarktrechtlichen Aspekte durchleuchtet. Netz- und Informationssicherheit hat eine wachsende Bedeutung in unserer Wirtschaft und Gesellschaft. Sie ist auch eine wichtige Voraussetzung für die Schaffung eines verlässlichen Umfelds für den weltweiten Dienstleistungsverkehr. Die Einordnung von Bitcoins im Bereich der Netz- und Informationssicherheit wird analysiert.

Collection: Conference Proceedings IRIS 2015; Peer Reviewed – Jury
LexisNexis Best Paper Award of IRIS2015
Category: Articles
Field of law: E-Commerce
Region: Austria

Citation: Helgo Eberwein / Árpád Geréd, Bits Coins, in: Jusletter IT 26. Februar 2015 – IRIS

Inhaltsübersicht

1 Finanzrechtliche Einordnung von Bitcoins
1.1 Was sind Bitcoins?
1.2 Regelungsumfeld für Bitcoinanbieter in finanzrechtlicher Hinsicht
1.3 Die Regelungen der Financial Action Task Force
2 Bitcoins im Lichte der Cybersicherheitsgesetze
2.1 Einleitung — Warum gerade jetzt?
2.2 Europäische Union — Die Richtlinie
2.2.1 Überblick
2.2.2 Die wesentlichsten Maßnahmen
2.2.3 Die Zielgruppe
2.2.4 Die NIS-Richtlinie und Bitcoins
2.3 Deutschland — Das Gesetz
2.3.1 Überblick
2.3.2 Die wesentlichsten Bestimmungen
2.4 Österreich — Der Plan
3 Fazit
4 Literaturverzeichnis

1 Finanzrechtliche Einordnung von Bitcoins

[Rz 1] Die digitale Revolution hat in allen Lebensbereichen der modernen Welt Fuß gefasst. Die bargeldlose Zahlung ist von steigender Bedeutung.[1] Die Netz- und Informationssicherheit (NIS) hat eine wachsende Bedeutung in unserer Wirtschaft und Gesellschaft. Sie ist auch eine wichtige Voraussetzung für die Schaffung eines verlässlichen Umfelds für den weltweiten Dienstleistungsverkehr.[2] Der Fokus des vorliegenden Beitrages soll auf der Einordnung von Bitcoins im Bereich der NIS liegen.

1.1 Was sind Bitcoins?

[Rz 2] Bitcoins sind eine dezentralisierte, digitale Währung, die 2008 von einem anonymen Wissenschaftler, welcher unter dem Pseudonym Satoshi Nakamoto bekannt ist, beschrieben wurde. Im Gegensatz zu herkömmlichen Währungen wie Euro, Pfund oder Dollar existiert bei Bitcoins keine zentrale Verwaltungsstelle, die für die Echtheit und den tatsächlichen Wert gehandelter Währungseinheiten zuständig ist.[3] Damit sind Bitcoins kein staatlich anerkanntes Zahlungsmittel. Von Haus aus sind Bitcoins kein Zahlungsmittel. Der Bitcoin an sich benötigt ja kein ausgebendes Institut, doch gibt es natürlich zahlreiche Dienstleistungen im Umfeld der Bitcoin-Verwendung. Erst durch die Akzeptanz der Bitcoins zum Erwerb von Waren oder Dienstleistungen werden Bitcoins als Zahlungsmittel verwendet.

1 Vgl. Bachler/Nothegger, Format 49/2014, 25.

2 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union COM (2013) 48 final (NIS-Richtlinie) 2.

3 Kaes, Bitcoins: Technische Einleitung in Eberwein/Steiner (Hrsg.), Bitcoins 1.

1.2 Regelungsumfeld für Bitcoinanbieter in finanzrechtlicher Hinsicht

[Rz 3] Wo bleiben also die Rechts- und vor allem die Informationssicherheit? Um dem Thema den nötigen Raum zu geben, wird zunächst analysiert, ob und wenn ja, in welchem Ausmaß Bitcoinanbieter den bestehenden finanzrechtlichen Regulativen unterliegen und welche Folgen das in der Praxis für die vielen Bitcoinanbieter hat.

[Rz 4] Bitcoin ist eine virtuelle Währung, die weder der Regulierung noch der Aufsicht der FMA unterliegt. Geschäftsmodelle, welche Bitcoins zum Gegenstand haben, können jedoch eine Konzessionspflicht nach einer der FMA zum Vollzug zugewiesenen Rechtsvorschriften auslösen.[4] Bitcoins sind mangels essenzieller Voraussetzungen weder Geld noch E-Geld. Bitcoins sind auch keine Finanzinstrumente i.S.d. § 1 Z. 7 und 7 a BWG 103 oder § 1 Z. 6 WAG. Der gewerbliche Eigenhandel mit Bitcoins bedarf damit keiner BWG-Konzession, ebenso ist die Anlageberatung, Vermögensverwaltung, Annahme und Übermittlung von Aufträgen sowie der Betrieb eines Multilateralen Handelssystems (MTF) im Hinblick auf Bitcoins nach WAG konzessionsfrei. Zur Konkretisierung der zivilrechtlichen Pflichtenlage bei Bitcoin-Transaktionen können freilich die Wohlverhaltensregeln des WAG analog angewendet werden.[5]

[Rz 5] Bitcoins sind ferner keine Zahlungsinstrumente nach ZaDiG, wohl aber Zahlungsmittel nach § 1 Abs. 1 Z. 6 BWG. Veräußerung und Umtausch von Bitcoins erfüllen den Begriff der Verwaltung von Zahlungsmitteln, wofür bei gewerblicher Tätigkeit eine Berechtigung nach dem § 4 Abs. 1 BWG erforderlich ist (Gedanke des Anlegerschutzes). Dagegen ist das Inzahlungnehmen von Bitcoins regulatorisch nicht erfasst und somit konzessionsfrei.[6] Handelsplattformen werden laut der Finanzmarktaufsicht nicht reguliert und unterliegen keiner Aufsicht. Eine Handelsplattform kann jederzeit geschlossen werden, so mussten mehrere Handelsplattformen ihre Tätigkeit bereits wieder einstellen. Bei Schließung der Handelsplattformen, z.B. durch Insolvenz oder durch das Verbot des An- und Verkaufs und des Handels mit Bitcoins in einem Staat, besteht kein Rechts-, Einlagen- oder Anlegerschutz. Es gibt keinen zentralen Betreiber, welcher in Anspruch genommen werden kann.[7]

[Rz 6] Im Gegensatz hierzu scheint laut Benndorf eine Einordnung des Handels mit Bitcoins unter § 1 Abs. 4 BörseG am besten geeignet. Bitcoins erfüllen als bewegliche körperliche Sachen die Anforderungen an «geeignete Waren» i.S.d. § 1 Abs. 4 BörseG. Demnach betreiben BitcoinExchanges «allgemeine Warenbörsen» als «Börseunternehmen» i.S.d. § 2 Abs. 1 BörseG und benötigen für den Handel mit Bitcoins eine Konzession des BMWFW gem. § 2 Abs. 2 BörseG. Dies gilt nicht für Unternehmen, welche Bitcoins als Gegenleistung für andere Waren, im Rahmen eines Tauschgeschäftes akzeptieren oder Leistungen rund um Bitcoins anbieten. Ob diese Einordnung nun tatsächlich den Funktionsgehalt von Bitcoins am besten verkörpert, sei dahingestellt.[8] In Deutschland gelten Bitcoins nicht als Wertanlage, sondern als Zahlungsmittel.[9]

---

4 http://www.fma.gv.at/de/sonderthemen/information-zu-bitcoin.html (abgerufen am 25. Januar 2015).

5 Falschlehner/Klausberger, Zur finanzmarktaufsichtsrechtlichen Einordnung von Bitcoins in Eberwein/Steiner (Hrsg.), Bitcoins, 60.

6 Ebenda, 55, 60.

7 http://www.fma.gv.at/de/sonderthemen/information-zu-bitcoin.html (abgerufen am 25. Januar 2015).

8 Benndorf, Bitcoins Versuch der rechtlichen Entschlüsselung einer Kryptowährung, 81.

9 http://www.faz.net/aktuell/finanzen/devisen-rohstoffe/digitale-waehrung-deutschland-erkennt-bitcoins-als-privates-geld-an-12535059.html (abgerufen am 25. Januar 2015).

1.3 Die Regelungen der Financial Action Task Force

[Rz 7] Die Financial Action Task Force on Money Laundering (FATF)[10] befasst sich unter anderem mit der Ausarbeitung von Richtlinien zur Umsetzung der Standards und der Verfassung von Dokumenten zur «Best Practice» sowie mit Fragen der Typologie im Rahmen von Geldwäschereihandlungen.[11] Ziel dieser Regelungen war eine signifikante Ausweitung der Befugnisse der nationalen Finanzmarktbehörden hin zu einer gesamten Überwachung aller Zahlungsabwicklungen. In der EU führten diese Regelungen beispielsweise zur Richtlinie 2007/64/EG, der Zahlungsdiensterichtlinie.[12]

[Rz 8] Zum Zeitpunkt der Erstellung dieser Regelungen, welche den gesamten Zahlungsverkehr erfassen sollen, gab es noch keine Bitcoins. In einem Dokument vom Juni 2014 wird festgehalten, dass virtuelle Währungen einerseits die Grundlage für zukünftige Zahlungssysteme bilden und andererseits ein sehr starkes Instrument für terroristische Aktivitäten darstellen. Auch eine Kategorisierung der virtuellen Währung wird vorgenommen.[13]

2 Bitcoins im Lichte der Cybersicherheitsgesetze

2.1 Einleitung — Warum gerade jetzt?

[Rz 9] Während in den Jahren zuvor Medien bereits über Bedrohungen durch Viren, Würmer und Trojaner berichteten[14], war 2011 das Jahr, in welchem Cybersicherheit, vor allem durch Aktivitäten von Hackergruppen wie Anonymous[15] oder LulzSec[16] fast zum Dauerthema in den allgemeinen Medien wurden.

[Rz 10] Anonymous fiel bereits 2008 mit dem Project Chanology[17], einer konzentrierten Aktion gegen die in einigen Staaten als Religionsgemeinschaft anerkannte Sekte Scientology auf. En-

---

10 Die FATF ist eine internationale, zwischenstaatliche Organisation. Sie wurde von der G-8 gegründet und umfasst 36 Mitglieder, wovon 34 selbständige Staaten und 2 Regionalorganisationen (EU-Kommission und der Kooperationsrat der Golfstaaten) sind. Das Sekretariat der Organisation befindet sich in Paris, am Sitz der Organisation for Economic Cooperation and Development (OECD). Die Kernaufgabe der FATF besteht darin, internationale Standards im Bereich der Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung zu verfassen und deren effektive Umsetzung durch gesetzgeberische, regulatorische und operative Maßnahmen im Rahmen gegenseitiger Länderprüfungen (Mutual Evaluations) zu kontrollieren.

11 https://www.finma.ch/d/finma/internationales/gremien/Seiten/fatf.aspx; http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatf-recommendations.html (abgerufen am 25. Januar 2015).

12 http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32007L0064 (abgerufen am 25. Januar 2015).

13 http://www.fatf-gafi.org/topics/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html; http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (abgerufen am 25. Januar 2015).

14 Beispielsweise über den Loveletter-Virus, siehe etwa http://www.sueddeutsche.de/digital/zehn-jahre-i-love-you-wurm-liebesvirus-mit-fatalen-folgen-1.941683 oder http://www.symantec.com/security_response/writeup.jsp?docid=2000-121815-2258-99 (abgerufen am 25. Januar 2015).

15 Siehe z.B. http://de.wikipedia.org/wiki/Anonymous_%28Kollektiv%29 (abgerufen am 25. Januar 2015) mit einer Zusammenfassung der wesentlichen Aktivitäten.

16 Siehe z.B. http://de.wikipedia.org/wiki/LulzSec (abgerufen am 25. Januar 2015) mit einer Zusammenfassung der wesentlichen Aktivitäten.

17 Siehe z.B. http://www.welt.de/vermischtes/weltgeschehen/article106612886/Anonymous-bekaempft-das-maechtige-Scientology.html (abgerufen am 25. Januar 2015).

de 2010 folgten DDoS-Attacken[18] gegen die Schweizer Postfinanz, Mastercard und Visa[19], doch erst die Hackerangriffe auf das Playstation-Netzwerk von Sony im April 2011[20], welche im Diebstahl der Daten von mehr als 70 Millionen Nutzern gipfelten, lenkte die Aufmerksamkeit der Öffentlichkeit auch auf die umgangenen Sicherheitsmaßnahmen, statt allein auf die Ideologien[21] der Beteiligten.[22] 2011 und 2012 folgten auch in Österreich medienwirksame Hackerangriffe, beispielsweise auf die Freiheitliche Partei Österreichs (FPÖ)[23] sowie die Gebühren Info Service GmbH (GIS)[24], von welcher etwa 214.000 Kundendaten kopiert wurden.

[Rz 11] 2013 enthüllte Edward Snowden die weltweiten Bespitzelungsaktivitäten seines ehemaligen Arbeitgebers, des US-amerikanischen Geheimdienstes National Security Agency (NSA).[25] Diese Aktivitäten, über welche die Medien ausführlich berichteten, machten der Öffentlichkeit bewusst, dass Cyberbedrohungen nicht nur von privaten Gruppierungen, sondern auch von (fremden) staatlichen Organisationen ausgehen können.

[Rz 12] In diesem Umfeld präsentierten Anfang 2013 sowohl die EU, als auch Deutschland Rechtsakte zur Cybersicherheit. Selbst wenn Sicherheit in der IT bereits zuvor sowohl von der EU, als auch von Mitgliedstaaten thematisiert wurde[26], so ist es sicherlich auch den zunehmenden öffentlichkeitswirksamen Hackerangriffen zu verdanken, dass Prävention und Maßnahmen in diesem Bereich nunmehr normiert werden sollen, statt weiterhin auf rein freiwillige Zusammenarbeit zu bauen.

---

18 Das ist die Blockade von Internetdiensten, beispielsweise mittels Überlastung von Infrastruktursystemen durch eine größeren Anzahl von Anfragen, als diese Systeme verarbeiten können, oder durch Ausnutzung von Programmfehlern, mittels derer Fehlfunktionen des Systems bis hin zum Absturz herbeigeführt werden. Siehe dazu z.B. auch http://de.wikipedia.org/wiki/Denial_of_Service (abgerufen am 25. Januar 2015).

19 Siehe z.B. http://www.spiegel.de/netzwelt/web/operation-payback-hacker-grossangriff-auf-mastercard-visa-co-a-733520.html (abgerufen am 25. Januar 2015).

20 Siehe z.B. http://www.spiegel.de/netzwelt/gadgets/attacke-auf-playstation-netzwerk-hacker-stehlen-millionen-sony-kundendaten-a-759161.html; oder http://www.extremetech.com/gaming/84218-how-the-playstation-network-was-hacked (abgerufen am 25. Januar 2015).

21 Sowohl die Kampagne gegen Scientology, also auch die Angriffe gegen Schweizer Postfinanz, Mastercard und Visa waren, zumindest offiziell, primär ideologisch und netzpolitisch motiviert. Diese Hintergründe wurden auch in den Medien näher ausgeführt.

22 Im Gegensatz zu den Berichten über die früheren Aktivitäten von Anonymous und LulzSec konzentrierten sich die Medien nun auch auf die betroffenen Nutzer und die Auswirkungen, welche die Angriffe auf diese haben.

23 Siehe z.B. http://diepresse.com/home/techscience/internet/sicherheit/677088/FPOHomepage_Pony-statt-Strache und http://diepresse.com/home/politik/innenpolitik/1269841/Anonymous-hacken-erneut-FPOWebsite- (abgerufen am 25. Januar 2015).

24 Siehe z.B. http://derstandard.at/1310511899361/ORF-Gebuehren-Homepage-der-GIS-von-Anonymous-gehackt oder http://kurier.at/lebensart/technik/gis-beugt-sich-anonymous-ultimatum/717.017 (abgerufen am 25. Januar 2015).

25 Gute Zusammenfassungen und Details zu diesem sogenannten «NSA-Skandal» finden sich z.B. auf http://www.taz.de/!119094/ oder http://www.theguardian.com/us-news/the-nsa-files (abgerufen am 25. Januar 2015).

26 So wurde beispielsweise die Europäische Agentur für Netz- und Informationssicherheit (ENISA) 2004 gegründet (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:l24153). Deutschland gründete das BSI bereits 1990 (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/BSI/bsiges_pdf.pdf?__blob=publicationFile) und publizierte ihre Cyber-Sicherheitsstrategie für Deutschland am 14. März 2011 (http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf) (abgerufen am 25. Januar 2015).

2.2 Europäische Union — Die Richtlinie

2.2.1 Überblick

[Rz 13] Am 7. Februar 2013 präsentierte die Europäische Kommission die Cybersicherheitsstrategie der EU[27] gemeinsam mit einem Vorschlag für eine Richtlinie über «Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union»[28], auch Netz- und Informationsrichtlinie oder NIS-Richtlinie genannt.

[Rz 14] Laut Begründung des Richtlinienvorschlags wurde im Zeitraum vom 23. Juli bis zum 15. Oktober 2012 Online-Konsultation zur «Verbesserung der Netz- und Informationssicherheit in der EU» durchgeführt. Nach dieser hatten 57% der Konsultationsteilnehmer 2011 Cybersicherheitsvorfälle «mit ernsten Auswirkungen auf ihre Tätigkeiten»[29] zu verzeichnen. Mit der NIS-Richtlinie verfolgt die EU daher das Ziel, einen unionsweit hohen gemeinsamen Netz- und Informationssicherheitsstandard zu schaffen. Zugleich soll das Vertrauen der (potentiellen) Nutzer in Online-Dienste gestärkt werden. Der Richtlinienvorschlag erwähnt dazu die Eurobarometer-Erhebung zur Cybersicherheit 2012[30], nach welcher 38% der Internetznutzer in der EU Bedenken in Bezug auf die Sicherheit von Online-Zahlungen haben und infolge dieser Bedenken ihr Verhalten bei der Nutzung von Online-Diensten wie etwa e-Commerce oder e-Banking geändert haben.

[Rz 15] Bemerkenswert ist die Schlussfolgerung der Europäischen Kommission, dass die Ist-Situation «das Ergebnis des bislang rein freiwilligen Vorgehens» ist und «keinen ausreichenden EU-weiten Schutz vor NIS-Vorfällen und NIS-Risiken»[31] bietet. Daher sollen Marktteilnehmer, die Dienste in der EU bereitstellen, sowie die öffentliche Verwaltung verpflichtet werden, ihre Cyber-Abwehrbereitschaft zu erhöhen und die Zusammenarbeit im Bereich der Cybersicherheit zu verbessern.

2.2.2 Die wesentlichsten Maßnahmen

[Rz 16] Vorauszuschicken ist, dass die NIS-Richtlinie gemäß Art. 2 ausdrücklich nur der Mindestharmonisierung, wenngleich auf hohem Niveau, dienen soll. Die Mitgliedstaaten sind daher nicht daran gehindert, höhere Sicherheitsstandards oder zusätzlich Maßnahmen vorzusehen.

- Nationale NIS-Strategie und nationaler NIS-Kooperationsplan (Art. 5): Die Mitgliedstaaten sind zur Annahme einer Strategie und eines Kooperationsplans im Bereich der Cybersicherheit verpflichtet.[32]
- Für die Netz- und Informationssicherheit zuständige nationale Behörde (Art. 6): Die nationale Behörde ist mit angemessenen technischen, finanziellen und personellen Ressourcen auszustatten. Sie ist überwacht die Anwendung der NIS-Richtlinie auf nationaler Ebene, trägt zu ihrer einheitlichen Anwendung in der Union bei und arbeitet auch mit den nationalen

[27] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_de.pdf (abgerufen am 25. Januar 2015).

[28] RL 2013/0027 (COD), http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_de.pdf (abgerufen am 25. Januar 2015).

[29] RL 2013/0027 (COD) 2.

[30] http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_fact_de_de.pdf (abgerufen am 25. Januar 2015).

[31] RL 2013/0027 (COD) 3.

[32] Diese müssen beispielsweise allgemeine Maßnahmen zur Abwehrbereitschaft, Reaktion und Wiederherstellung und einen Risikobewertungsplan zur Bestimmung der Risiken und zur Bewertung der Auswirkungen potenzieller Sicherheitsvorfälle enthalten.

Strafverfolgungs- und Datenschutzbehörden zusammen.[33]

- Kooperationsnetz (Art. 8): Die zuständigen Behörden und die Kommission bilden ein Netz für die Zusammenarbeit bei der Bewältigung von Cybersicherheitsrisiken und —vorfällen.
- Sicherheitsanforderungen und Meldepflicht (Art. 14): Die öffentliche Verwaltung und Marktteilnehmer haben «geeignete technische und organisatorische Maßnahmen» zu ergreifen, um «die Risiken für die Sicherheit der Netze und Informationssysteme, die ihnen unterstehen und die sie für ihre Tätigkeiten nutzen, zu managen».[34]
- Normung (Art. 16): Um eine einheitliche Umsetzung des Art. 14 zu gewährleisten, müssen die Mitgliedstaaten die Anwendung einschlägiger Normen fördern, zu denen die Kommission eine Liste erstellen wird.
- Sanktionen (Art. 17): Die Mitgliedstaaten müssen Sanktionen vorsehen, die «wirksam, angemessen und abschreckend» sind, um die Anwendung der NIS-Regeln zu gewährleisten.

2.2.3 Die Zielgruppe

[Rz 17] Von der NIS-Richtlinie sollen gemäß Art. 3 Abs. 8 «Marktteilnehmer», das sind «Anbieter von Diensten der Informationsgesellschaft» (lit. a) sowie «Betreiber kritischer Infrastrukturen» (lit. b) erfasst sein. Nach der nicht erschöpfenden Aufzählung in Anhang II der NIS-Richtlinie wären das z.B. Plattformen des elektronischen Geschäftsverkehrs, Internet-Zahlungs-Gateways, Strom- und Gasversorger, Luftfahrtunternehmen oder Kreditinstitute. Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG[35] sind von den Sicherheitsanforderungen und der Meldepflicht ausgenommen.

[Rz 18] Auch wenn Bitcoins bislang in keinem Mitgliedstaat der EU als elektronisches Geld — welches sich begrifflich und rechtlich von Zahlungsmitteln unterscheidet — anerkannt sind und Bitcoins-Börsen daher keiner finanzmarktrechtlichen Regulierung unterliegen, wären durch diese Regelung auch Bitcoins-Börsen als Plattformen des elektronischen Geschäftsverkehrs von der NIS-Richtlinie erfasst. Ob dies auch so bleibt, ist aber fraglich. Das Europäische Parlament hat in der ersten Lesung am 13. März 2014 den Kommissionsvorschlag zwar grundsätzlich angenommen, in seiner Entschließung[36] aber stark modifiziert.[37]

---

[33] Im Kooperationsnetz werden Frühwarnungen zu Sicherheitsrisiken herausgegeben, die weiterreichend sind oder mehrere Mitgliedstaaten betreffen können.

[34] Die Eignung der Maßnahmen ist dabei jeweils nach dem Stand der Technik und dem bestehenden Risiko zu beurteilen. Der Fokus der Maßnahmen soll nach der NIS-Richtlinie nicht nur auf der Schadensprävention, sondern auch auf der Gewährleistung der Kontinuität der Dienste liegen. Sicherheitsvorfälle sind nach Maßgabe der zuständigen Behörde zu melden.

[35] Somit Unternehmen mit weniger als 10 Mitarbeitern und maximal €{} 2 Mio. Jahresumsatz. Siehe auch http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:de:PDF (abgerufen am 25. Januar 2015).

[36] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0244+0+DOC+XML+V0//DE (abgerufen am 25. Januar 2015).

[37] Die vom Parlament vorgeschlagene Version konzentriert sich allein auf Betreiber kritischer Infrastrukturen und lässt Dienste der Informationsgesellschaft wie auch die öffentliche Verwaltung ausgeklammert. Gleichzeitig wurde aber die Liste der Betreiber kritischer Infrastrukturen erweitert, beispielsweise um organisierte Handelssysteme des Finanzmarkts und Internet-Knoten. Als nächster Schritt im Gesetzgebungsverfahren steht die erste Lesung im Rat der EU aus.

2.2.4 Die NIS-Richtlinie und Bitcoins

[Rz 19] Diese Handelsplattformen sind von den Nutzern, welche Bitcoins kaufen oder verkaufen, zu unterscheiden. Der einzelne Nutzer der Bitcoins kann als Konsument gesehen werden. Die Handelsplattform ist mit einer Bank vergleichbar, die Nutzer der Plattform mit den Kunden dieser Bank.[38] Nach Art. 3 Abs. 8 Buchstabe a des Entwurfes der NIS-Richtlinie sind «Anbieter von Diensten der Informationsgesellschaft» solche Anbieter, die die Bereitstellung anderer Dienste der Informationsgesellschaft ermöglichen Anhang II enthält eine nicht erschöpfende Liste solcher Anbieter. So werden in Ziffer 1 des Anhangs II Plattformen des elektronischen Geschäftsverkehrs genannt. Deshalb sind Handelsplattformen nicht als Infrastrukturbetreiber, sondern als Diensteanbieter einzuordnen. Sollten Dienstanbieter daher — wie vom EU-Parlament vorgeschlagen — nicht reguliert werden, wäre Bitcoin-Handelsplattformen nicht von der NIS-Richtlinie umfasst.

2.3 Deutschland — Das Gesetz

2.3.1 Überblick

[Rz 20] Am 12. März 2013 präsentierte die deutsche Bundesregierung ihren ersten «Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme», das IT-Sicherheitsgesetz[39]. Dieses wird kein eigenes Gesetz sein, sondern bestehende Gesetze, allen voran das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), novellieren. Der aktuelle Entwurf wurde am 17. Dezember 2014 von der Bundesregierung beschlossen.

[Rz 21] Obwohl die Erläuterungen zum IT-Sicherheitsgesetzt, im Gegensatz zur Begründung des Richtlinienvorschlags, auf diesen Punkt nicht eingehen, würde mit diesem Gesetz das derzeit etablierte Meldeverfahren im Rahmen der erst 2012 gegründeten Allianz für Cybersicherheit[40] abgeschafft werden.

2.3.2 Die wesentlichsten Bestimmungen

[Rz 22] Im Gegensatz zur NIS-Richtlinie erfasst das IT-Sicherheitsgesetz gemäß § 8a nur Betreiber kritischer Infrastrukturen, wobei Kleinstunternehmer wieder ausgenommen sind. Die Definition entspricht im Wesentlichen jener der NIS-Richtlinie. Welche Betreiber aber letztendlich betroffen sind, legt gemäß § 10 das Bundesministerium des Innern per Verordnung fest.

[Rz 23] Gemäß § 8a müssen Betreiber kritischer Infrastrukturen binnen 2 Jahren nach Inkrafttreten der vorgenannten Verordnung angemessene organisatorische und technische Vorkehrungen zur Absicherung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer Systeme treffen. Auch hier ist der Stand der Technik zu berücksichtigen wobei Angemessenheit vorliegt, wenn der erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Infrastruktur steht. Der Nachweis der Erfüllung die-

[38] Auch eine Einzelperson, welche eine hohe Anzahl an Bitcoins besitzt und Bitcoinminer, welche versuchen Bitcoins erzeugen, erbringen im Gegensatz zu Miningpoolbetreibern keine Dienste.

[39] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?__blob=publicationFile (abgerufen am 25. Januar 2015).

[40] Die Allianz für Cyber-Sicherheit ist eine Initiative des BSI in Zusammenarbeit mit dem BITKOM mit derzeit mehr als 1000 Teilnehmern. Siehe auch https://www.allianz-fuer-cybersicherheit.de (abgerufen am 25. Januar 2015).

ser Verpflichtung ist zumindest alle 2 Jahre «auf geeignete Weise» nachzuweisen, beispielsweise durch Sicherheitsaudits, Prüfungen oder Zertifizierungen. Das BSI muss damit nicht mehr die Angemessenheit der Maßnahmen selbst prüfen sondern vielmehr die Angemessenheit der verwendeten Prüf- und Zertifizierungsverfahren.

[Rz 24] Erhebliche Sicherheitsvorfälle, die zu einem Ausfall oder einer Beeinträchtigung geführt haben oder hätten führen können sind von den Betreibern nach § 8b an das BSI zu melden. Nachdem betroffene Unternehmen erfahrungsgemäß Sicherheitsvorfälle nach Möglichkeit lieber verschweigen, als über diese unter Namensnennung zu berichten[41], wurde die Möglichkeit einer pseudonymen Meldung durch eine Kontaktstelle oder einer brancheneigenen Ansprechstelle vorgesehen.

[Rz 25] Das BSI ist nach § 8b zentrale Meldestelle für alle. Es kann Warnungen sowohl an betroffene Kreise, als auch an die Öffentlichkeit herausgeben. Zudem kann es auch Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen. Bemerkenswert ist die Befugnis des BSI gemäß § 7a informationstechnische Produkte und Systeme auch vor Markteinführung zu untersuchen. Vor Veröffentlichung der gewonnenen Erkenntnisse ist aber dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben. Auffällig ist das Fehlen jeglicher Sanktionen.

2.4 Österreich — Der Plan

[Rz 26] Am 20. März 2013 präsentierte die Bundesregierung die neue Österreichische Strategie für Cyber Sicherheit.[42] Am 16. Mai 2014 folgte sodann die Ankündigung eines Cyber-Sicherheits-Gesetzes. Von diesem Gesetz existiert bislang zwar noch kein Entwurf, es kann aber davon ausgegangen werden, dass das geplante Gesetz auch umgesetzt werden wird.

[Rz 27] Cybersicherheitsinitiativen gibt es in Österreich bereits seit 2002, als von der ISPA und dem Bundeskanzleramt aus Anlass des 2000 verbreiteten Loveletter-Virus die Computer Incident Response Coordination Austria (CIRCA) geschaffen wurde. 2008 wurden die Agenden von CIRCA vom neu geschaffenen Computer Emergency Response Team (CERT) sowie dem Government Computer Emergency Response Team (GovCERT) übernommen. Die Hauptaufgabe beider CERTs ist die Sammlung von Informationen zu Sicherheitsvorfällen, welche bislang allein auf freiwilliger Basis gemeldet werden, die Koordinierung der Reaktionen und die Herausgabe sicherheitsrelevanter Meldungen.

[Rz 28] Im Dezember 2014 führte das Kuratorium Sicheres Österreich (KSÖ) unter Beteiligung u.a. der CERTs und des Bundesministeriums für Inneres eine Cybersecurity-Übung durch. Die Koordinierung wurde, gewissermaßen als Generalprobe, vom geplanten Cyber-Security-Center (CSC) des Bundesministeriums für Inneres übernommen. Die Übung zeigte, dass die Zusammenarbeit zwischen staatlichen und privaten Teilnehmern zwar gut funktionierte, jedoch ein CSC unumgänglich war. Daher soll dieses bereits 2015 in Probebetrieb gehen. Ebenso zeigte die Übung Defizite bei den rechtlichen Rahmenbedingungen, weil oft unklar war, ob bestimmte In-

[41] Die ursprünglich von der deutschen Bundesregierung vorgesehene Berichtspflicht mit Namensnennung wurde beispielsweise mit diesem Argument kritisiert.

[42] Österreichische Strategie für Cyber Sicherheit http://www.bundeskanzleramt.at/DocView.axd?CobId=50748 (abgerufen am 25. Januar 2015).

formationen aus rechtlicher Sicht geteilt werden dürfen oder nicht. Die Einführung eines Cyber-Sicherheits-Gesetzes erweist sich damit als unumgänglich.[43]

3 Fazit

[Rz 29] Bitcoin-Börsen scheinen sich derzeit, zumindest was die bevorstehenden rechtlichen Regelungen zur IT-Sicherheit betrifft, in einer sehr gemütlichen Position zu befinden: Mangels Anerkennung von Bitcoins als elektronisches Geld und nachdem sich ein Trend abzuzeichnen scheint, (einstweilen) nur Betreiber kritischer Infrastrukturen den Cybersicherheitsgesetzen zu unterwerfen, ist die Chance eher gering, dass sie die neuen IT-Sicherheitsregeln einhalten müssen.

[Rz 30] Gänzlich außer Acht lassen sollten sie die neuen Regelungen aber nicht. Das nicht allein, weil die nationalen Behörden Meldungen und Empfehlungen ausgeben können, welche auch außerhalb kritischer Infrastrukturen von Relevanz sind. Viel relevanter ist das Kriterium der Angemessenheit der ergriffenen Sicherheitsmaßnahmen, bei dem nicht allein auf den Stand der Technik, sondern auf das potentielle Risiko abgestellt wird, ohne Berücksichtigung finanzieller Faktoren. Wiewohl dieses Kriterium nicht für alle Unternehmen verbindlich sein wird, hat es doch das Potential zu einer neuen Auslegungsregel für die Eignung ergriffener IT-Sicherheitsmaßnahmen, besonders in Branchen, die mit relativ hochwertigen elektronischen Gütern handeln.

4 Literaturverzeichnis

Bachler, Martina/Nothegger, Barbara, Bye-bye, Bares! Format 49/2014, 25 ff.

Benndorf, Laurenz, Bitcoins Versuch der rechtlichen Entschlüsselung einer Kryptowährung, Diplomarbeit Universität Graz (2014).

Bundeskanzleramt Österreich (Hrsg.), Österreichische Strategie für Cyber Sicherheit, Bundeskanzleramt Österreich, Wien (2013).

Bundesministerium des Innern (Hrsg.), Cyber-Sicherheitsstrategie für Deutschland, Bundesministerium des Innern, Berlin (2011).

Eberwein, Helgo/Steiner, Anna Zoe (Hrsg.), Bitcoins, Jan Sramek Verlag, Wien (2014).

Helgo Eberwein, Jurist, Bundesministerium für Inneres[1], Abteilung III/4, Aufenthalts-, Personenstands- und Staatsbürgerschaftswesen, Herrengasse 7, 1014 Wien, AT, helgo.e@web.de
Árpád Geréd, Rechtsanwalt, Maybach Görg Lenneis Geréd Rechtsanwälte GmbH, Museumstraße 5, 1070 Wien, AT, a.gered@mglp.eu, http://www.mglp.eu
Der Beitrag gibt ausschließlich die persönliche Meinung des Autors wieder und ist weder als Äußerung im Rahmen der Dienstpflicht noch als Rechtsauffassung der Behörde zu verstehen.

[43] http://www.bmi.gv.at/cms/bmi/_news/bmi.aspx?id=436E3444473136415A41593D&page=0&view=1 (abgerufen am 25. Januar 2015).