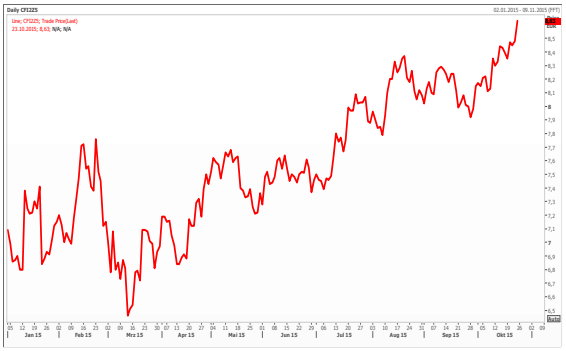
- CO_2 Monitoringkonzept- und Berichterstellung
- CO_2 Registerkontoführung für Unternehmen
- CO_2 Emissionsrechte Kauf/Verkauf EUA/aEUA, CER/ERU
- CO_2 Emissionsrechte Tausch, Spot- und Forwardhandel
- CO_2 Portfoliomanagement und Strategieberatung
- EEG Befreiungsanträge, Strompreiskompensation und Energieoptimierung
- Infos unter Freecall 0800-590 600 02



EUA DEC15 01.01.2015 bis 23.10.2015 Quelle: ICE London

Emissionsbrief 11-2015

Praktische Informationen zum Emissionshandel

Ausgabe vom 26.10.2015

Cyberkriminalität beim Onlinebanking könnte auch Sicherheit im Unionsregister gefährden - 3-Jahres-Aktualisierungen laufen

Unkorrekte Handlungen von Bevollmächtigten im Register können bei einem nicht ausreichend sicheren mTAN-Verfahren die Möglichkeit eines Zertifikate-Diebstahls ermöglichen. Durch die in letzter Zeit bekannt gewordenen Betrugsserien im Onlinebanking mit gestohlenen mobilen TAN-Nummern (mTAN) stellt sich die Frage, inwieweit Zertifikate auf Konten des Unionsregisters noch sicher sind, wenn gleichzeitig durch Bevollmächtigte eines Anlagenbetreibers gegen Regelungen der Registerverordnung verstoßen wird. Emissionshändler.com® untersucht in seinem hier vorliegenden Emissionsbrief 11-2015 die Möglichkeiten und Abläufe, die zu einem eventuell erfolgreichen Cyberdiebstahl von Zertifikaten (wie schon in 2010 geschehen) führen würden.
Weiterhin berichten wir über die laufenden Aufforderungen der DEHSt zur Aktualisierung von Daten, die für die (damalige) Eröffnung des Anlagenkontos des Betreibers notwendig waren sowie von Personendaten der entsprechenden Bevollmächtigten.
Weiterhin geben wir in einem Fremdbeitrag von BBH eine Übersicht über den Stand der Finanzmarktrichtlinie MiFID II wider und wie sich diese auf Anlagenbetreiber, Händler und Stadtwerke auswirken würde.

Erneuter Zertifikate-Klau von Registerkonten eventuell nur noch eine Frage der Zeit

Der Zertifikate-Klau von CO2-Registerkonten scheint nach neuesten Meldungen über Sicherheitslücken im mTan-Verfahren nicht mehr unmöglich zu sein. Insbesondere dann nicht, wenn sich die Kontobevollmächtigten des Registerkontos gar nicht oder nicht vollständig an die Regeln der Registerverordnung 389/2013 halten.
Ein möglicher Schaden hierbei kann durchaus um ein vielfaches höher sein, als die jetzt bekannt gewordenen Fälle von Cyber-Diebstählen von bis zu 30.000 Euro, die Kunden der Telekom auf ihren Bankkonten hinnehmen mussten.
Dass diese Opfer bisher ihre Schäden ersetzt bekamen, lag wohl daran, dass diese in aller Regel keine Schuld trifft bzw. diese höchstens einmal fahrlässig gehandelt hatten, indem sie keinen optimalen Virenschutz auf ihrem PC hatten.
Diese Praxis der Erstattung des Schadens würde jedoch nach Einschätzung von Emissionshändler.com® bei einem Pishing auf einem Zertifikatekonto so gut wie ausgeschlossen sein, da hierbei im Falle eines Cyber-Diebstahl auch ein vorsätzlicher Verstoß eines Bevollmächtigten gegen die Registerverordnung vorliegen wird. Dies ist nach den Erfahrungen von Emissionshändler.com® durchaus üblich, so dass es nur eine Frage der Zeit sein wird, bis es zu entsprechenden Pishing-Attacken auf Registerkonten kommt, bei denen dann die Bevollmächtigten nach einem Schaden voll in der persönlichen Haftung stehen.

Das mTan-Verfahren zeigt Sicherheitslücken

In den letzten Wochen ist es in Deutschland zu einer Pishing-Serie beim Onlinebanking gekommen. Wie mehrere Medien berichteten, haben Betrüger in höherer Anzahl jeweils fünfstellige Beträge von den Bankkonten von Kunden abgebucht, wobei mehrere Banken betroffen waren und der Gesamtschaden bisher bei mehr als einer Million Euro liegt.

Das 2-Kanal-Authenifizierungsverfahren mit PC und Mobilfunkgerät (welches so auch im CO2-Unionsregister eingesetzt wird) galt bisher als sicher, da die von einem System generierte mTan über das Mobilfunkgerät eingeht, und somit unabhängig von einem eventuell mit einem Trojaner infizierten PC ist.

Nach nun fast 5 Jahren der fast problemlosen Nutzung des mTans-Verfahrens sind nunmehr kriminelle Profis am Werk, die mit hoher krimineller Energie und technischer Kompetenz vorgehen. Bisher betroffen sind Kunden verschiedener Banken, die jedoch immer nur Handyverträge mit der Telekom gehabt haben sollen und mit dem mTan-Verfahren arbeiten.

Die Vorgehensweise der Betrüger erfolgte in mehreren Schritten

Zuerst wurde mit einem Trojaner (Spähsoftware) in den Computer des Opfers eingedrungen. Hier wurde der Zugang zum Online-Konto mit dem zugehörigen Passwort gesucht. Schon hier im PC oder über andere Wege sind dann anschließend die Mobilnummer des Opfers sowie eventuelle Kundenpasswörter beschafft worden, die für die Authentifizierung beim Provider benötigt werden könnten.
Anschließend übernahmen die Betrüger gegenüber der Telekom die Identität eines Mitarbeiters eines Mobilfunk-Shops und beantragen im Namen des Kunden für eine angeblich verlorene Karte die Freischaltung einer Blanko-SIM Karte (die in manchen Shops physisch ständig verfügbar sind) bzw. auch die Zusendung einer SIM-Ersatzkarte an die „Adresse des Shops“.

Nach Freischaltung der Blanko-Karte bzw. Erhalt der Ersatzkarte mit der Telefonnummer des Opfers nehmen sie dann die Geld-Transaktion vor, von der das Opfer entweder nichts oder später etwas mitbekommt.
Hierbei kann nun die Methode der doppelten SIM-Karte zum Einsatz kommen. Dabei verwendet der Täter eine sogenannte Multi-SIM-Karte, also eine Karte, die unter der gleichen Handynummer ausschließlich SMS empfangen kann, ohne dass die bisherige SIM-Karte abgeschaltet werden muss. Aus Sicht des Opfers ist scheinbar alles in Ordnung, es kann problemlos telefonieren, aber es kommen eventuell für eine kurze Zeit von ein paar Minuten keine SMS an, was nicht weiter auffällt.
Hat sich der Täter jedoch für die Methodik einer normale SIM-Ersatzkarte entschieden, so kann dies dem Opfer schon wesentlich eher auffallen, da mit dem Einsetzen der Ersatzkarte in das Handy des Täters die SIM-Karte des Opfers nicht mehr funktioniert. Es kann nicht mehr telefonieren und simsen und bekommt auch keine Gespräche und SMS mehr.

Aktuelle Gegenmaßnahmen und weitere Methoden der Täter

Zwischenzeitlich konnte erfahren werden, dass die Telekom Maßnahmen zur SIM-Karten Ausgabe und zur Identifikation von Händlern und Shop Betreibern eingeleitet hat, die einen solchen Betrug unterbinden sollen. Hierzu zählt insbesondere die zur Verfügung Stellung von Blankokarten an Shopbetreiber und die postalische Versendung an Kunden, was dann wieder den Briefkasten der Kunden für die Betrüger interessant werden lässt.
Sicherlich kann man davon ausgehen, dass zwischenzeitlich auch schon andere Mobilfunkprovider mit „erfundenen Shop-Identitäten“ betroffen sind. Selbst wenn dies nicht der Fall sein sollte und sich die anderen Provider der Branche mit ähnlichen Sicherheits-maßnahmen schützen würden, so werden sich kriminellen Banden immer neue Ideen einfallen lassen, um weiter mit dem mTan-Verfahren abkassieren zu können.
So war bereits 2014 bekannt geworden, dass Smartphones, die mit dem Android-Trojaner FakeToken infiziert sind, von Betrügern in die Lage versetzt werden können, mTans abzugreifen, damit dann die Kriminellen die Konten des Handybesitzers leer räumen können.
Seit dem 24. Oktober 2015 wurde nun auch öffentlich, dass nach einer Meldung des Portals Heise Security es Forschern der Uni Erlangen gelang, die mTan-App der Sparkasse zu knacken, Geldbeträge umzuleiten und nach Belieben deren Höhe zu verändern.

Der Cyber-Diebstahl von Zertifikaten ist nunmehr (wieder) möglich geworden

Der zukünftige Diebstahl von CO2-Zertifikaten im Unionsregister wird unter Berücksichtigung der bisher bekannt gewordenen kriminellen Aktivitäten rund um das mTan-Verfahren immer wahrscheinlicher.

Hierbei muss noch einmal wiederholt werden, dass die damaligen Pishing-Attacken Anfang des Jahres 2010 in verschiedenen nationalen CO2-Registern nur möglich waren, weil es noch kein 2-Kanal-Authentifizierungs-system gab und auch weil ein 4-Augen-Prinzip noch nicht eingeführt worden war.

Im heutigen Unionsregister mit dem vorgeschalteten ECAS Authentifizierungssystem ist der Sicherheits-standard im Prinzip ausreichend. Dies ist jedoch nur dann der Fall, wenn das 2-Kanal-Verfahren und das 4-Augen-Prinzp vollständig und korrekt eingehalten werden.

Davon ausgehend, dass es nunmehr nicht mehr unmöglich ist, dass das mTan-Verfahren von kriminellen Betrügern manipuliert wird, sollte bei Kontoinhabern und Bevollmächtigten ihre vorhandene Sicherheitsarchitektur und ihre internen Ablaufprozesse in den Fokus rücken.

Wie könnte ein Cyber-Diebstahl von Zertifikaten im Unionsregister ablaufen?

Insbesondere dürfte die Möglichkeit zukünftiger erfolgreicher Attacken darin begründet werden, dass folgende Verhaltensweisen bei Registerkonto Bevollmächtigten vorliegen können:

a) Bevollmächtigter A ist alleine im Betrieb und nutzt (mit Einverständnis des Bevollmächtigten B) den Zugang und das Diensthandy des zweiten Bevollmächtigten.

b) Bevollmächtigter A ist alleine im Betrieb, der Bevollmächtigte B ist krank oder ausgeschieden und nutzt (mit oder ohne Einverständnis des Bevollmächtigten B) den Zugang und das Diensthandy des zweiten Bevollmächtigten.

c) Die Bevollmächtigten A und B nutzen ihre Zugänge über ein und denselben PC.

d) Die Bevollmächtigten A und B haben den gleichen Mobilfunkbetreiber (z. B. Telekom) und nutzen ihre Zugänge zeit- und teilweise über ein und denselben PC.

Davon ausgehend, dass einer der PCs der Bevollmächtigten mit einer Schadsoftware infiziert ist, würde es nach bisherigen Erkenntnissen möglich sein, dass durch einen kriminellen Betrüger eine unberechtigte Transaktion angestoßen wird.

In den Fällen c) und d) würde dies dazu führen, dass der zweite Bevollmächtigte den ersten Bevollmächtigten anspricht, was denn diese Transaktion bedeuten könnte, die er bestätigen soll. Im schon unwahrscheinlichen Falle, dass einer oder beide der PCs infiziert sind und das Smartphone des zweiten Bevollmächtigten mTans unberechtigt weiterleitet, würde bereits eine bestätigte Transaktion ausgelöst.

Schaut man sich jedoch die obigen Punkte a) und b) an, so kann dieses unkorrekte Verhalten dazu führen, dass durch die Aufhebung des 4-Augen-Prinzips eine bestätigte Transaktion durch unbefugte Dritte gestartet wird. Da hierbei die Bevollmächtigten auch keine SMS auf ihr Handy bekommen bleibt die einzige Chance, dass durch die dann ausgelösten Mailbestätigungen des Unionsregisters der oder die Bevollmächtigten rechtzeitig innerhalb der 26-Stunden-Transaktionsfrist reagieren.

Fazit zur Sicherheit von mTan im Unionsregister

Tatsache ist, dass das Risiko und der potenzielle Schaden beim Missbrauch von mTans im CO2-Register wesentlich höher sein können, als bei einem Pishing im Onlinebanking. Dies schon deswegen, weil es bei Zertifikatetransaktionen keine Höchstgrenzen gibt und weil eine einmal durchgeführte Transaktion unwiderruflich ist. Im Normalfalle ist hingegen die Wahrscheinlichkeit eines erfolgreichen Zertifikate-Klaus immer noch sehr niedrig, sofern sich alle beteiligten Bevollmächtigten an die Regeln der Registerverordnung halten.

Infobox
Das CO2-Konto-Paket im rechtskonformen Emissionshandel

Das CO2-Konto-Paket von Emissionshändler.com® befreit das Unternehmen weitgehend von hohen Risiken, die bei einer nicht ordnungsgemäßen Kontoführung bestehender Bevollmächtigter bzw. durch technisches oder menschliches Versagen eintreten können.

Der Ausfall von Kontobevollmächtigten (BV) und/oder deren Technik wird durch die Einsetzung eines externen Kontobevollmächtigten von Emissionshändler.com® kompensiert, der ebenso auch die administrativen und gesetzlichen Termine überwacht sowie die vorhandenen Bevollmächtigten des Unternehmens bei der Navigation in der sich oftmals durch Updates verändernden Registersoftware unterstützt.

Detaillierter Leistungsinhalt zum CO2-Konto-Paket unter Freecall 0800-59060002 oder per Mail unter info@emississionshaendler.com

Sollte jedoch ein bestimmtes Verhalten um sich greifen, wonach durch Bevollmächtigte vorsätzlich gegen den Artikel 34 (1), Punkte a)-c) verstoßen wird und durch

einen unberechtigten Zugang zum Register und/oder durch einen Identitätsmissbrauch das 4-Augen-Prinzip ausgehebelt wird, darf sich ein Betreiber über einen eingetretenen Schaden nicht beklagen. Dass sich dieser wiederum mit seinen Haftungsansprüchen an seine Bevollmächtigten wenden kann, wird in der Regel finanziell kaum etwas bringen.
Wesentlich sinnvoller scheint es hier, schon im Vorfeld das Risiko zu minimieren, indem einer der Bevollmächtigten z. B. einem externen Dienstleister angehört und außerdem noch Zugänge zu unterschiedlichen Mobilfunkprovidern genutzt werden (siehe auch Infobox Seite zuvor).

==========

Nicht rechtzeitige Aktualisierungen können mit Sperrungen von Bevollmächtigten und von Registerkonten geahndet werden

Wie den meisten Anlagenbetreibern bekannt, trat zum 02.05.2013 die neue Registerverordnung 389/2013 in Kraft. Diese VO ersetzte wesentliche Teile der vorherigen Verordnung und regelte im Wesentlichen die Bestimmungen des bereits ein Jahr zuvor zum Juni 2012 eingeführten Unionsregisters, welches die nationalen Register abgelöst hatte. Einer der wichtigsten Bestimmungen der VO regelt hierbei die Aktualität aller Angaben.
Die allermeisten Anlagenbetreiber verfügten zum Zeitpunkt der Einführung des neuen Unionsregisters zum Juni 2012 bereits über ein nationales Betreiberkonto, welches damals fast automatisch in das Unionsregister überführt wurde. Einzige Voraussetzung war nur, dass die Mobilfunknummer eines Bevollmächtigten noch einmal in einer Prozedur bestätigt werden musste.
Nunmehr greift mit dem Artikel 25 (4) spätestens seit Juli 2015 eine der wesentlichsten Regeln der VO 389, der den nationalen Registerbehörden vorschreibt, innerhalb eines 3-Jahres-Zeitraums viele Angaben rund um das Registerkonto zu überprüfen.
Dies sind neben der schon erwähnten **Aktualität** auch Bestimmungen zur **Vollständigkeit**, zur **Richtigkeit** sowie zur **Exaktheit** der entsprechenden Daten. Überprüft werden die Daten und Angaben:

- zur Anlage
- zum Ansprechpartner der Anlage
- zum Kontoinhaber
- zu den Bevollmächtigten des Registerkontos

Sicherlich mögen sich im Einzelfall die nationalen Registerbehörden an diese 3-Jahres-Frist bei einigen Betreibern gehalten haben, jedoch bekommen zumindest die allermeisten Kontoinhaber und Bevollmächtigten im Deutschen Register erst seit dem Sommer 2015 - und damit bereits außerhalb der 3-Jahres-Überprüfungsfrist - eine entsprechende Aufforderung der DEHSt.
Dies dürfte im Einzelfall den einen oder anderen Rechtsspezialisten in späterer Zukunft vielleicht einmal beschäftigen, sofern ein Anlagenbetreiber einmal einen Schaden geltend machen würde, der auf eine nicht fristgemäße Überprüfung seiner Angaben durch die Behörde zurückzuführen wäre, wie konstruiert sich ein solcher Schaden auch immer darstellen würde.
In jedem Falle ist es jedoch anscheinend üblich, dass von Kontoinhabern und Bevollmächtigte innerhalb der 3-Jahres-Frist vereinzelt initiierte Aktualisierungen gemäß Artikel 25 (4) von den Behörden nicht gern gesehen werden, da diese sich ihren Arbeitsprozess der systematischen Abfrage der Daten ungern stören und durcheinanderbringen lassen möchten.
So gesehen hat ein Anlagenbetreiber und seine Bevollmächtigten die Wahl, ob diese darauf verzichten von sich aus in einer 3-Jahres-Frist beglaubigte Personalpapiere, Führungszeugnisse, Handelsregister-auszüge etc. an die Behörde zu senden oder sich korrekt an den Absatz 4 des Artikel 25 zu halten, der regelt, dass die Behörde die Initiative innerhalb von 3 Jahren ergreift, um die Aktualisierung durchzuführen.

Welche Daten werden innerhalb 3 Jahren mindes-tens einmal überprüft?

Der Handelsregisterauszug

In der Regel werden Kontoinhaber per Mail aufgefordert, einen aktuellen **Handelsregisterauszug** ihrer Gesellschaft zu erbringen, aus dem die Vertretungsregelungen der Gesellschaft und die vertretungsberechtigten Personen ersehen werden können. Hierbei ist in der Regel ein elektronischer Auszug des jeweiligen Amtsgerichts ausreichend. Der Handelsregisterauszug darf hierbei nicht älter als 3 Monate sein.

Das Führungszeugnis

Ein aktuelles **Führungszeugnis** der Kontobevoll-mächtigten - welches nicht älter als 3 Monate sein darf - muss alle 3 Jahre vorgelegt werden. Hierbei wird ein privates Führungszeugnis bevorzugt, da dieses von der ausstellenden Behörde an die Privatadresse des Antragstellers gesendet wird.
Sollte der Bevollmächtigte seinen ständigen Wohnsitz im Ausland haben, dann wird von der nationalen Registerbehörde in vielen Fällen eine extra beglaubigtes Führungszeugnis verlangt, welches zudem noch beglaubigt in die Landessprache übersetzt werden muss.

Der Ausweis oder der Pass

Da nationale Ausweisdokumente und Pässe in der Regel alle 10 Jahre ablaufen, erhalten die Inhaber mit ihrem

neuen Ausweisdokument auch eine andere Ausweis- oder Passnummer.
Schon aus diesem Grunde ist die nationale Registerbehörde verpflichtet, gemäß VO389, Anhang VIII in Verbindung mit Artikel 25 (4) die Aktualität der Angaben innerhalb einer 3-Jahres-Frist zu kontrollieren und den Bevollmächtigten ggf. aufzufordern, ein neues Ausweisdokument vorzulegen.
Aus dem Ausweisdokument muss mindestens neben dem Namen, Vornamen, Geburtsort, Geburtsdatum und der Gültigkeitsdauer auch die Anschrift des ständigen Wohnsitzes sowie die Unterschrift des benannten Kontobevollmächtigten hervorgehen, ggf. auch zusätzlich durch eine Meldebestätigung.
Zu erwähnen wäre, dass die Art der Übermittlung (elektronisch oder Papier) und der Sicherheitsstandard (beglaubigt oder unbeglaubigt) gemäß VO389 oftmals im Ermessen der nationalen Registerbehörde liegt, die hier im Einzelfall auch auf einer Beglaubigung durch eine Meldebehörde oder einen Notar bestehen kann.

Die ToDos für den Kontobevollmächtigten

Nachdem ein Bevollmächtigter turnusmäßig innerhalb eines 3-Jahres-Zeitraumes von seiner Registerbehörde per Mail angeschrieben worden ist und die geforderten Unterlagen beschafft hat, muss er diese entweder per VPS oder per Briefpost an die Registerbehörde senden. Nachdem diese die Papiere geprüft und er eine Bestätigung per Mail erhalten hat, dass die Prüfung positiv verlaufen ist, wird er auch aufgefordert, seine persönlichen Daten zu aktualisieren, insbesondere die Art des Ausweisdokumentes Ausweis/Pass und dessen ID-Nummer. Dies ist aus der Perspektive des Bevollmächtigten vor allem dann nicht ganz logisch, wenn er zuvor eben diese Daten der Behörde übermittelt hatte. Hierzu muss man jedoch wissen, dass die Aktualisierung der Ausweisdaten nicht im Registermenü der Bevollmächtigten vorgenommen werden muss, sondern auf der Startseite oben links unter der URID-Nummer des Bevollmächtigten, wozu nur der Bevollmächtigte einen Zugang hat.

Angaben zur Person werden über den Link im Startmenü oben links aktualisiert

Kommt der Bevollmächtigte dieser Aktualisierung nicht in angemessener Zeit nach, so wird die Behörde zunächst eine beglaubigte Ausweiskopie verlangen und wenn auch diese nicht erbracht wird, den Bevollmächtigten vom Kontozugang aussperren.

Besondere ToDos für den Kontoinhaber

Da nunmehr seit dem Juni 2012 das Unionsregister in Betrieb ist und auch ein kompletter 3-Jahres-Zeitraum für die „Überprüfung der Angaben zur Kontoeröffnung“ verstrichen sind, sollten Kontoinhaber den Artikel 25 (1) besonders ernst nehmen. Dieser schreibt ihnen vor, dass sie innerhalb 10 Tagen eine Änderung von Daten und Angaben zur Anlage und deren Ansprechpartner mitteilen, die sich eventuell geändert haben könnten.
Welche Daten dies betreffen könnte, ist aus dem Anhang VI-I und dem Anhang VI-II zu ersehen. Es sind dies insgesamt 32 mögliche Daten, von denen theoretisch sich bis zu 30 geändert haben können. Nur die Anlagenkennung und das Datum der Genehmigung der Anlage sind unveränderbar.
Dies kann in der Praxis bedeuten, dass eine nicht fristgemäße Mitteilung innerhalb 10 Tagen über z. B. die Änderung einer Telefonnummer eines Ansprechpartners gemäß Artikel 34 (2) Punkt e) zu einer Kontosperrung - mit allen weiteren Konsequenzen - führen kann.

==========

Mit freundlicher Genehmigung der **Kanzlei Becker Büttner Held** dürfen wir in diesem Infobrief den folgenden Auszug aus dem Energiehandels-Newsletter der Kanzlei vom 14.10.2015 abdrucken:

MIFID I und II – Entwicklungen, Stand und Ausblick

Während die praktische Umsetzung der REMIT in vielen Häusern das aktuelle Umsetzungsthema ist, wird die Entwicklung der Finanzmarktregulierung, insbesondere der novellierten Finanzmarktrichtlinie (MiFID II), nicht weniger gespannt verfolgt, da hier entschieden wird, ob komplette Geschäftsmodelle künftig noch fortgeführt werden könnten.
Die MiFID II ist im vergangenen Jahr zwar auf den Weg gebracht worden. Es steht aber noch die nationale Umsetzung an. Und auf europäischer Ebene werden die Diskussionen um die für den Energiehandel zentrale Definition der Warenderivate (Punkt I.) und die Gestaltung der Nebentätigkeitsausnahme (Punkt II.)geführt.

I. Die Derivatedefinition

Einer der Kernpunkte der Finanzmarktrichtlinie ist die in ihrem Anhang I Abschnitt C enthaltene Auflistung

von Finanzinstrumenten. Dabei gilt es zu beachten, dass dies nicht nur hinsichtlich der Definition der (Waren-)Derivate im Zusammenhang mit der MiFID II gilt, sondern auch mit der MiFID I.

1. Warenderivate nach MIFID I

Zur Auslegung der Warenderivate unter C6 und C7 der MiFID I hat die europäische Aufsichtsbehörde ESMA Anfang Mai 2015 Guidelines veröffentlicht. Damit soll eine einheitliche, konsistente Auslegung und Verwendung gewährleistet werden, insbesondere um auch eine einheitliche Auslegung mit der EMIR zu erzielen – wohlgemerkt: rund elf Jahre nach Veröffentlichung der MiFID! Zur Erinnerung: Ein Warenderivat liegt vor, wenn es sich um ein Termingeschäft handelt und wenn es entweder an einer Börse oder über eine sog. multilaterale Handelsplattform (MTF – Multilateral Trading Facility) geschlossen wird oder wenn es finanziell erfüllbar ist (also vertraglich anstelle der Lieferung auch ein finanzieller Ausgleich vorgesehen ist). Deshalb sind im Umkehrschluss physische Lieferungen im OTC-Handel regelmäßig aufsichtsfrei, da sie keine Finanzinstrumente darstellen.

Nicht ganz eindeutig war, was denn unter physischer Erfüllung („physically settled“) zu verstehen ist. Genau hierzu hat sich ESMA in ihren Guidelines nun geäußert. Insoweit hat ESMA nun bestätigt, dass jedenfalls Forwards, die an einem regulierten Markt oder über ein MTF geschlossen werden, in den Anwendungsbereich der MiFID I fallen. Zudem hat ESMA klargestellt, dass „physically settled“ dann vorliegt, wenn

- eine tatsächliche physische Lieferung erfolgt,
- das Eigentumsrecht durch ein entsprechendes Dokument übertragen wird (z. B. Lieferschein, Lagerschein) oder
- anderweitig ein Eigentumsübergang auch ohne tatsächliche Lieferung erfolgt; klassischerweise sind dies Fahrplangeschäfte.

2. Warenderivate nach MIFID II

Das gilt für MiFID I; nicht aber für die MiFID II. Denn bei dieser sieht die Richtlinie vor, dass es entsprechende delegierte Rechtsakte der Kommission geben soll. Zur Vorbereitung dieser Rechtsakte hatte ESMA zuletzt einen Technical Advice veröffentlicht, d. h. eine Gesetzgebungshilfestellung für die Kommission. Darin soll ESMA den Begriff „physically settled“ für Energiegroßhandelsprodukte ausdrücklich definieren – und ESMA geht dabei einen Schritt weiter als in ihrem MiFID I-Papier: Ihr Vorschlag sieht vor, dass es für das „physische Settling“ u. a. auf sog. „proportionate arrangements“ der Handelspartner zu Produktion bzw. Verbrauch ankommen soll. Für Handelspartner, die sich auf eine physische Lieferung berufen möchten, ist dies von erheblicher Bedeutung. Denn sie haben unbedingt dafür Sorge zu tragen, dass die physische Lieferung zu ihren (industriellen) Aktivitäten, ihren Produkten, ihrer Speichermöglichkeit bzw. ihrem Verbrauch passt. Würde diese Vorgabe nachteilig ausgelegt, wäre die Folge, dass z. B. ein Energieversorgungsunternehmen nur so viel einkaufen dürfte, wie es auch an seine Endkunden liefern kann, bzw. nur so viel auf dem Großhandelsmarkt verkaufen darf, wie es erzeugen kann.

Das Thema ist für die Energieunternehmen so brisant, weil daran die (sektorspezifische) Erleichterung der Derivatedefinition hängt. Wie Sie wissen, sollen ja künftig nach der MiFID II auch die sog. organisierten Handelsplattformen (OTF) also auch die kleineren Brokerplattformen – unter die Aufsichtspflicht fallen. D. h. jedes über ein OTF geschlossene Termingeschäft gilt als Derivat und wird damit ein aufsichtspflichtiges Finanzinstrument. Für den Energiebereich wurde letztlich eine Ausnahme aufgenommen: Ausgenommen von der OTF-Erweiterung werden ausdrücklich REMIT-Geschäfte, jedoch nur, wenn sie ausschließlich physisch zu erfüllen sind.

Nebenbei: ESMA hat nun erstmals bekanntgegeben, wie viele Derivate eigentlich in Europa genutzt werden, denn insoweit sind die Trade Repositories, die die EMIR-Meldungen entgegen-nehmen, aufgefordert, aggregierte Daten hinsichtlich der offenen Positionen, die Transaktionsvolumen sowie die Werte pro Derivateklasse zu veröffentlichen. Hieraus ergibt sich, dass seit Meldebeginn im Februar 2012 mehr als 16 Milliarden Datenübermittlungen erfolgten, d. h. ca. 300 Millionen pro Woche; Stand: 29.05.2015). Die Daten, sortiert nach den groben Assetklassen, können auf den Websites der Trade Repositories eingesehen werden. Die Zahlen beziehen sich also auf sämtliche Warenderivate, nicht nur auf Energie (oder gar Strom oder Gas).

II Nebentätigkeitsausnahme

Wie Sie wissen, wird es die – von den meisten Unternehmen der Energiebranche genutzte – Nebentätigkeitsausnahme in der jetzigen Form in der MiFID-II-Welt nicht mehr geben. Diese wird künftig eingeschränkt. Sie kann dann nicht mehr genutzt werden, wenn es um die Ausführung von Kundenaufträgen („executing client orders“) geht. Insoweit sieht zwar Erwägungsgrund 25 der Mi-FID II vor, dass diese Einschränkung nicht zur Anwendung kommt, wenn es für beide Parteien letztlich eine Nebentätigkeit ist. Allerdings wird es darauf ankommen, wie dieser Grundgedanke in das nationale Recht umgesetzt wird.

Zur Frage, wie Haupttätigkeit und Nebentätigkeit voneinander abzugrenzen sind, soll die europäische Aufsichtsbehörde ESMA Regulatory Technical Standards verfassen. Hierzu hatte ESMA im Dezember 2014 und dann im Frühjahr 2015 einen Vorschlag veröffentlicht und zur Konsultation eingeladen. Während ESMA anfangs vorschlug von einer Nebentätigkeit auszugehen, wenn die Tätigkeit insgesamt „weniger als 50 %“ der Gesamttätigkeit ausmache, reduzierte ESMA diese Schwelle dann auf „5 %“. Das sorgte zunächst für Unmut und Verunsicherung bei Unternehmen, die fürchteten, zukünftig unter die Regulierung zu fallen.
Nachdem der ESMA die Bedenken mitgeteilt wurden, verkündete sie bei einer Anhörung im Europäischen Parlament im Juni 2015, dass man wesentliche Verbesserungen im ESMA-Vorschlag bezüglich der Nebentätigkeitsausnahme erwarten könne. Diese kann man inzwischen im Entwurf vom 28.09.2015 nachlesen. Danach ist ein zweistufiger Test vorgesehen: Zu-nächst muss der Gesamtmarkt betrachtet werden, d. h. die Unternehmensaktivität wird mit der Aktivität im gesamten Markt verglichen. Als zweite Stufe findet ein Test auf Gruppenebene statt, d. h. die Handelsintensität bzw. „Spekulationsintensität“ des Unternehmens. Für die Frage, ob noch eine Nebentätigkeit vorliege, kommt es danach – kurz gesagt – darauf an: Je mehr ein Unternehmen macht, desto kleiner darf sein Marktanteil sein.
Das heißt zunächst einmal: Unternehmen müssen auf Gruppenbasis prüfen, wie groß die Aktivitäten in Derivaten sind, die nicht zu Hedgingzwecken genutzt werden, im Verhältnis zum Gesamtderivateanteil. Je nachdem wie groß diese Aktivität ist, hat dies wiederum Auswirkungen auf die Schwelle des ersten Tests; sobald die Aktivität mehr als 10 % ausmacht, halbiert sich der Schwellenwert des ersten Tests, bei mehr als
50 % darf die Aktivität des Unternehmens im Vergleich zum Markt nur noch weniger als 1/5 des Schwellenwertes des ersten Tests ausmachen.
Der so ermittelte Wert ist dann ins Verhältnis zur Aktivität im Markt zu setzen, wobei die Unternehmen ihre gesamten Derivate zusammenzählen, ihre Absicherungsgeschäfte aber rausrechnen können. Für jede Asset-Klasse gibt es unter-schiedliche Schwellen, für Strom liegt diese bei 6 % und für Gas bei 3 %.
Diese Werte sind aber noch nicht in Stein gemeißelt: die Kommission hat jetzt drei Monate Zeit, die Vorschläge von ESMA zu prüfen. Danach sind das Europäische Parlament und der Rat zu beteiligen. Es bleibt also weiterhin spannend.

Disclaimer

Dieser Emissionsbrief wird von der GEMB mbH herausgegeben und dient ausschließlich zu Informationszwecken. Die GEMB mbH gibt weder juristische noch steuerliche Ratschläge. Sollte dieser Eindruck entstehen, wird hiermit klargestellt, dass dies weder beabsichtigt noch gewollt ist.
Die GEMB mbH übernimmt keine Gewähr für die Richtigkeit und Vollständigkeit der Informationen oder ihre Geeignetheit zu einem bestimmten Zweck, weder ausdrücklich noch stillschweigend Dieser Brief wird auch nicht mit der Absicht verfasst, dass Leser eine Investitionsentscheidung, eine Kauf- oder Verkaufs-entscheidung hinsichtlich eines CO2-Produktes oder Markt- und/oder eine Vertragsentscheidungen in jeglicher anderer Hinsicht tätigen. Alle hier gezeigten Preiskurven basieren auf Daten der ICE-London, generiert aus einem Reuters-Informationssystem.

Unser Angebot

Kontakten Sie uns einfach unverbindlich unter 030-398 8721-10 oder Freecall 0800-590 600 02 sowie per Mail unter info@emissionshaendler.com oder informieren Sie sich im Internet über weitere Leistungen unter www.emissionshaendler.com.

Herzliche Emissionsgrüße
Ihr Michael Kroehnert

Verantwortlich für den Inhalt:
Emissionshaendler.com®
GEMB mbH, Helmholtzstraße 2-9, 10587 Berlin
HRB 101917 Amtsgericht Berlin Charlottenburg, USt-ID-Nr. DE 249072517
Telefon: 030-398872110, Telefax: 030-398872129
Web: www.emissionshaendler.com , www.handel-emisjami.pl
Mail: info@emissionshaendler.com
Mitglied im Vorstand Bundesverband Emissionshandel und Klimaschutz BVEK www.bvek.de