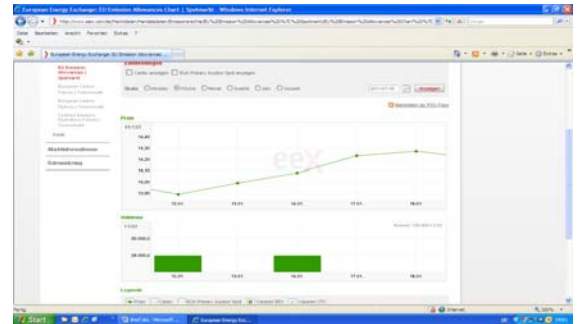




- Zakupimy dla Państwa CO2 na giełdzie
- Sprzedamy Państwa CO2 na giełdzie
- Doradzimy przy zawieraniu umów Forward
- Dokonamy dla Państwa wymiany EUA/CER/ERU; CER/CER
- Zarządzamy certyfikatami EUA i CER



Handl Spot sparaliżowany

Quelle: EEX

## 2011-01 News-emisje CO2

### Informacje z praktyki w handlu emisjami

Wydanie z 24.01.2011

## W UE-handel emisjami sparaliżowany- austriackie rezerwy EUA skradzione - Za pomocą zagrożenia wybuchem bomby zdobyte dane klientów rejestru - Konto handlowca z 475.000 EUA opróżnione

Po miliardowych oszustwach podatkowych związanych z podatkiem VAT, fauszywych certyfikatów CER na Węgrzech, milionowych stratach spowodowanych kradzieżą certyfikatów oraz danych klientów, europejski handel emisjami coraz bardziej przybliża się do krawędzi chaosu.

Trzeci tydzień kalendarzowego 2011 nie zostanie przez wielu uczestników rynku, odpowiedzialnych na giełdach oraz w krajowych rejestrach, a przede wszystkim przez Komisję UE zbyt szybko zapomniany.

Nastąpił skoncentrowany i zakończony powodzeniem atak na infrastrukturę informatyczną rejestrów krajowych, na konta operatorów, na konta krajowe oraz na dane klientów rejestru. Wydarzenia te - zwłaszcza niewystarczające zabezpieczenia IT wielu rejestrów krajowych - zmusiła Komisję do wstrzymania handlu spot w UE, aby opanować sytuację określaną jako prawie chaotyczną.

Emissionshändler.com w **News-emisje 01-2011** przedstawia chronologiczny przegląd wydarzeń oraz ukazuje możliwe przyczyny katastrofy.

### Austriacki rejestr online zaatakowany, 10 stycznia - skradzione rezerwy narodowe EUA

12 stycznia na stronie internetowej rejestru opublikowano, początkowo stosunkowo niegroźną informację, o następującej treści:

*Federalny Urząd Ochrony Środowiska GmbH jako siedziba rejestru oraz ECRA GmbH jako serwis rejestru pragną poinformować, że z powodu ataku hakerskiego w dniu 10.01.2011, ze względu na bezpieczeństwo będą musiały być zamknięte wszystkie dostępy do austriackiego rejestru handlu emisjami, oraz że rejestr nie jest dostępny do odwołania.*

Zarówno dwa dni wcześniej, jak i w wiele dni po opublikowaniu powyższej informacji, nie było wiadomo o tym, jaki skandal wydarzył się 10 stycznia.

W ubiegły piątek, 21 stycznia (11 dni później!), na konferencji prasowej ECRA poinformowano o tym, że 10 stycznia poprzez atak hakerów skradzione zostały rezerwy narodowe Austriackiego Rejestru Handlu Emisjami, w ilości 488.141 EUA.

Kilka minut przed dokonaniem kradzieży dokonany został atak cybernetyczny, tak zwany DOS (Denial of Service), który sparaliżował system informatyczny urzędu. Atak taki polega na zalaniu systemu IT taką ilością zapytań i informacji, aby system zajęty ich przetwarzaniem, nie mógł dalej wykonywać swojej pracy, aby coraz bardziej go spowolnić lub np. doprowadzić do awarii.

Według ECRA osoby oraz konta rejestrowe prowadzących instalacje nie zostały dotknięte atakiem cybernetycznym. Wychodząc z założenia, że urzędnicy upoważnieni do dysponowania narodową rezerwą znajdującą się na koncie, chronią dane dostępowe, nasuwa się pytanie, na ile bezpieczny jest system rejestrowy oraz jego otoczenie IT w krajach członkowskich.

Według przedstawiciela urzędu, nielegalnie przetransferowane certyfikaty zostały w międzyczasie odnalezione w Lichtensztajnie i w Szwecji, gdzie zostały one zamrożone na kontach do momentu pozytywnego rozpatrzenia wniosku o dokonanie



transferu zwrotnego, co ma uzasadnienie prawne ale jednocześnie nie jest pewne.

Interesujące jest stanowisko austriackiego urzędu, który zapewnia, że zostało dokonane wszystko, aby zabezpieczyć bezpieczeństwo kont. Powoływano się przy tym na regularną aktualizację oprogramowania, która „w tym przypadku okazała się niewystarczającą”. Również rejestr w Wiedniu jest zdania, że wszystkie poprzez Komisję UE narzucone standardy zostały zachowane.

Wtajemniczeni w Brukseli żartują już z Komisji: **„Zniknięcie certyfikatów stanowiących rezerwę narodową w drastyczny sposób pokazuje, jak źle- w porównaniu do rynków finansowych- chroniony przed kradzieżą i oszustwem jest handel emisjami”** (źródło: Dow Jones).

Jak w międzyczasie wiadomo, atak z 10.01.2011 był tylko próbą generalną przed „napadem” na konta czeskich operatorów.

### **18 stycznia, poprzez zagrożenie podłożenia bomby, skradziono dane klientów czeskiego rejestru**

W międzyczasie, od 19 stycznia do południa 22 stycznia, kiedy uczestnicy handlu emisjami CO2 próbowali rozwiązać zagadkę związaną z przypadkiem Blackstone (kradzież 475.000 EUA), przedstawicielowi odpowiedzialnemu za czeski rejestr (względnie prywatnej firmie OTE AS upoważnionej do zajmowania się rejestrem) stawało się coraz bardziej jasnym, że od kilku dni mają pewien „problem”. Problem ten został zakomunikowany całej Europie w piątek, 21.01.2011:

Już we wtorek, 18.01.2011 OTE AS przerażona była anonimową informacją o podłożeniu bomby, skierowanej przeciwko rejestrowi CO2.

Informacja ta doprowadziła do ewakuacji budynku, w którym znajduje się infrastruktura IT rejestru. Po tym, jak w ciągu 5 godzin policyjne poszukiwania materiału wybuchowego były bezskuteczne, współpracownicy świadczący usługi OTE SA mogli powrócić na swoje miejsca pracy.

W piątek 21.01.2011 właściwy urząd nie potwierdził, czy pracownicy po powrocie na swoje miejsca pracy stwierdzili jakiegokolwiek nieprawidłowości w działaniu systemu, czy też nie.

Faktem wydaje się jednak, że podczas nieobecności pracowników najprawdopodobniej „ściągnięte” zostały częściowo lub całkowicie dane dotyczące klientów rejestru oraz ich dane dostępowe. Dlaczego nie zostało to zauważone, względnie natychmiast zakomuni-

kowane klientom oraz opinii publicznej, pozostaje na razie tajemnicą komunikacyjną czeskiego rejestru. W każdym razie faktem jest, że rejestr pozostał otwarty dla wszystkich transakcji, co w końcu doprowadziło do kradzieży certyfikatów z kont klientów (jak dowiedziano się później).

Dowodem niedoskonałości rejestru jest fakt, że firma usługowa w dziedzinie CO2 Blackstone, w dniu następnym musiała poinformować urząd o tym, że z jej konta zniknęły wszystkie 475.000 certyfikatów.

Według dwóch informatorów, którzy nie chcą ujawniać swoich danych, możliwym jest, że opróżnione zostały konta znacznie większej ilości klientów, nie tylko Blackstone. Również administrator odpowiedzialny za serwis OTE dla rejestru okazuje się w dniu 21.01.11 bezradny w stosunku do branży Dow Jones: „do tej pory nie jest wyjaśnione, czy również z innych kont zostały skradzione certyfikaty”.

Ciekawe jest, w jakich kawałkach prawda, związana z tym przypadkiem, ujrzy światło dzienne.

### **Blackstone, polsko-czeski usługodawca w dziedzinie CO2, w dniu 19 stycznia zgłasza kradzież 475.000 certyfikatów ze swojego konta**

W środowe przedpołudnie 19.01.11 Nikos Tornikidis, menadżer Blackstone Global Venture- usługodawca w dziedzinie CO2, podczas codziennego sprawdzania swojego konta handlowego CZ-121-256-0, nie wierzy własnym oczom. Certyfikaty wszystkich klientów, którymi -jak mówi strona internetowa- jego firma zarządza, zniknęły .

Po dokładnym zbadaniu stało się jasnym, że na podstawie transakcji o numerze CZ12753, już w dniu poprzednim, punktualnie o 11.00, certyfikaty przekazane zostały na nieznane jemu konto w Polsce.

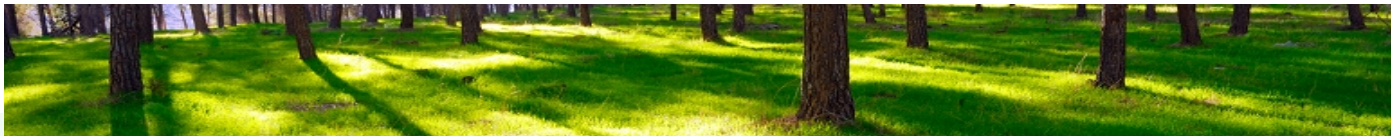
Tornikidis przekazuje informację do czeskiego rejestru, któremu w dniu poprzednim skradzione zostały dane klientów, którzy nie zostali o tym poinformowani.

Wspólnie ustalono, że certyfikaty zdążyły już opuścić polskie konto oraz, że transferowane są w kierunku Estonii, a stamtąd do Lichtensztajnu.

Ile z 475.000 certyfikatów EUA dotarło do oazy podatkowej w Lichtensztajnie, dla dobra śledztwa nie zostało przez tamtejszy rejestr ujawnione. Oczekiwać można jednak, że nie jest to ich całkowita ilość.

Chociaż na pierwszy rzut oka wydawać się może, że powodem kradzieży była nieudolność oraz braki w systemie IT rejestru (jak już miało to miejsce w Austrii), to wiele wskazuje na to, że w tym przypadku nie wszystko przebiegało tak, jak zakładano.

Nasuwa się pytanie, dlaczego menadżer takiego usługodawcy, przez równe 24 godziny, nie sprawdza swojego konta oraz nie przeprowadza żadnych



transakcji. Z doświadczenia Emissionshändler.com® jest to mało prawdopodobne, jako że przynajmniej raz dziennie stan konta powinien być sprawdzany oraz ponieważ certyfikaty wchodzące na konto oraz z niego wychodzące rozpoznają stan konta, szczególnie w przypadku, gdy jest on nagle równy zeru.

Dalej postawić można pytanie, dlaczego według informacji menadżera, kazał on sobie dostarczyć z rejestru listę skradzionych certyfikatów.

Jasnym jest, że każdy posiadacz konta powinien wiedzieć o tym, że wszystkie numery identyfikacyjne przekazanych certyfikatów odczytać można z dowodu przeprowadzenia transakcji, czyli że nie musi o to pytać rejestru. Zagadką pozostaje, dlaczego tak się nie stało. Faktem jest, że w ten sposób dokonujący kradzieży zyskał na czasie, aby certyfikaty EUA zamienić na pieniądze.

Jedną z mniejszych niezgodności odnośnie konta certyfikatów poszkodowanego usługodawcy jest fakt, że do odpowiedniego konta **rejestrowego CZ-121-256-0** nie jest przypisany żaden normalny adres mailowy. Kto dociekać będzie w rejestrze UE, znajdzie adres mailowy, który odsyła na dziwną stronę internetową w Melbourne/Australia. Przy takim zbiorze niewielkich niezgodności, można jako insider w handlu emisjami, stać się bezradnym albo też skierować przypuszczenia w innym kierunku.

**W związku z tym najbardziej irytującym jest fakt, że pośród skradzionych certyfikatów EUA znajdują się również takie, które już wcześniej zostały skradzione!** (patrz Infobox po prawej).

W każdym razie, przypadek certyfikatów skradzionych w środę 19.01.11 oraz ich (częściowo) możliwa do stwierdzenia droga przez Europę doprowadził do tego, że oprócz rejestru w Austrii, również rejestry w Czechach, Polsce, Estonii, Lichtensztajnie i Grecji zostały zamknięte.

Poza tym poinformowane zostały europejskie giełdy CO<sub>2</sub>, które okrężną drogą weszły w posiadanie listy certyfikatów skradzionych firmie Blackstone, jako że istniało duże niebezpieczeństwo, że niechcący skradzione certyfikaty CO<sub>2</sub> mogłyby zostać wprowadzone do obiegu.

#### **4. Atak hakerów na rejestry w Polsce i Estonii, milionowa kradzież w Rumunii**

W minionych dniach i tygodniach miały miejsce, uprzednio zapowiadane, ataki hakerów na konta rejestrowe w Polsce i Estonii (Źródło: Usługi branżowe

CO<sub>2</sub> Dow Jones). Wychodząc z założenia, że systemy IT w tych krajach nie są bezpieczniejsze niż przeciętna wszystkich 27 rejestrów europejskich, przyjąć można, że również tutaj skradzione zostały dane klientów, jeśli nie certyfikaty.

#### **Infobox**

#### **Ponad 13.000 skradzionych EUA w Rumunii zostały dwukrotnie (!) skradzione**

*Po tym jak w środę i czwartek 19/20 stycznia 2011 na giełdach CO<sub>2</sub> oraz wśród handlowców krążyła lista skradzionych certyfikatów Blackstone, każdy kto zechciał mógł tę listę z numerami certyfikatów porównać ze swoimi własnymi zasobami EUA.*

*Jako że Emissionshändler.com® posiada również listę 1,6 miliona certyfikatów skradzionych cementowni Holcim, podjął się trudu porównania tych list, co wykonywane ręcznie było bardzo żmudnym przedsięwzięciem.*

*Wśród skradzionych certyfikatów Holcim znajduje się między innymi blok numerów 2432694706-2432844705, odpowiadający ilości 150.000 certyfikatów.*

*Na liście Blackstone znajduje się prawie 60 różnych zakresów numerów z ponad 20 krajów, wśród których jeden, pochodzący z Rumunii, posiada zakres numerów 2432791606-2432804705.*

*Matematycznie daje to jednoznaczność 13.100 jednakowych liczb, a stąd 13.100 certyfikatów EUA z jednakowym blokiem numerów.*

**Oznacza nie mniej i nie więcej jak to, że Blackstone Global Ventures znajdował się w posiadaniu certyfikatów EUA pochodzących z kradzieży w Holcieniu, a teraz powtórnie ukradzionych.**

*Według informacji pochodzących od odpowiedzialnych za transakcje osób, certyfikaty mogą pochodzić jedynie z kupna na giełdzie spot Bluenext w Paryżu, co z pewnością udowodnione może być na podstawie protokołów z dokonanych transakcji.*

*Należy tutaj zauważyć, że tylko bardzo niewielu wtajemniczonym UE może być wiadomo, na jakiej zasadzie certyfikatom EUA, które opuszczają konto rejestrowe przyznawane są numery. Pewnym jest to że, jakie numery certyfikatów opuścić mogą konto w transakcji wyjściowej, nie może być określane przez pełnomocnika ustanowionego dla tego konta. Jest to zastrzeżone wyłącznie dla systemu rejestrowego, który nadaje numery i to nie przypadkowo, lecz na podstawie (nietypowej) zasady: **First in, Last out**. Oznacza to, że niektóre bloki numerów opuścić mogą konto jedynie wtedy, kiedy konto zostanie całkowicie opróżnione oraz, że istnieje bardzo duże przetarasowanie różnych oznaczeń krajowych na kontach aktywnych uczestników handlu, co z kolei bardzo utrudnia kontrolę zakresów numerów. Oznacza to również, że pozbycie się z konta, z jakiegokolwiek powodu, certyfikatów o konkretnych numerach, jest bardzo trudne.*



Na stronie internetowej polskiego rejestru KASHUE, od 20.01.11 znajduje się informacja, że do tej pory certyfikaty nie zostały skradzione.

Jednocześnie wskazuje się, że przy rozpoznaniu jakichkolwiek manipulacji w rejestrze podjęte zostaną „odpowiednie kroki ograniczające zagrożenie”. Najprawdopodobniej manipulacje takie już dawno miały miejsce.

Jako że w przeciwieństwie do Niemiec nie został jeszcze w Polsce i innych krajach wprowadzony podwójny sposób zatwierdzania transakcji ( numer TAN jako SMS na telefon komórkowy), operatorzy w Polsce będą musieli w ciągu najbliższych miesięcy być bardzo ostrożni oraz powinni codziennie kontrolować stan swoich kont.

Całkiem inny wymiar miała kradzież w listopadzie 2010. **Rumuńskiej cementowni Holcim** skradzionych zostało **1,6 miliona certyfikatów** poprzez tak zwany atak Phishing. Do chwili obecnej 600.000 certyfikatów pojawiło się na różnych kontach, pozostałej większości certyfikatów poszukuje w dalszym ciągu Rumuński Urząd do walki z terroryzmem oraz przestępczością zorganizowaną. Pasującym do tego jest przyznanie poprzez rejestr oazy podatkowej w Lichtensztajnie, w minionych miesiącach już kilkakrotnie odkryto na kontach skradzione certyfikaty. Zauważyć tutaj należy, że Lichtensztajn posiada tylko dwóch operatorów, co w tak małym kraju wydaje się normalne. Natomiast, jeśli spojrzeć na listę prawie 200 (!) handlowców (z kontem-121 ), można tylko ze zdumieniem przyglądać się fantastycznym nazwom „handlowców”.

### **W środę wieczorem o 19.00 (19.01.11) zostały zamknięte do odwołania wszystkie pozostałe rejestry CO2**

W środowe południe 19 stycznia- po tym, jak przypuszczalnie zgłoszone zostały ataki hakerów również na inne rejestry- Komisja UE została w końcu zmuszona do reakcji. W szczególności po tym, jak stwierdzono, że kradzież austriackich rezerw narodowych (oraz po podaniu tego do wiadomości) spowoduje w następnych dniach presję opinii publicznej, która już teraz poddaje w wątpliwość cały system handlu emisjami.

Poza tym, Dyrektor Generalny Działu Klimatycznego UE Jos Debelke, znajdował się coraz bardziej „pod ostrzałem”. Po kradzieży w rumuńskim Holcimiu (1,6 miliona EUA w listopadzie 2010), w dniu 03.12.2010 wydał on oficjalne oświadczenie, że zasadniczo każdy operator odpowiada za bezpieczeństwo swojego konta. W szczególności powiedział on, że UE nie widzi większych problemów związanych z bezpieczeństwem

systemów rejestrowych, ale że dłożone zostaną starania, systematycznie zwiększające to bezpieczeństwo. Oświadczenie z 03.12.2010 w oryginale na stronie <http://ec.europa.eu/environment/ets/>

Po eskalacji wydarzeń w ciągu 10 ostatnich dni, zarówno dla osób odpowiedzialnych w UE, jak też dla prowadzących rejestry w krajach członkowskich stało się jasnym, że na wszystkich poziomach systemu podjęte być muszą zdecydowane kroki.

Dotyczy to w szczególności poziomu organizacyjnego:

- Komisja UE
- Generalna Dyrekcja Klimatyczna EU
- Prowadzący rejestry krajowe
- Pełnomocnicy rejestrów krajowych
- Posiadacze kont rejestrowych (operatorzy, handlowcy, giełdy etc.)

Po tym jak stało się jasnym, że europejski system handlu CO2 ITS, w szczególności w Europie ale też na świecie, sam się zdyskredytował oraz stał niewiarygodnym, po południu w dniu 19.01.11 zdecydowano, że handel emisjami zostanie wstępnie wstrzymany do 26.01.11 oraz że zablokowane zostaną transakcje na kontach rejestrowych wszystkich krajów członkowskich, z wyłączeniem zwrotu certyfikatów do rejestrów krajowych (Oryginał oświadczenia z 19.01.11 na stronie <http://ec.europa.eu/environment/ets/> ).

Dodatkowo w piątek 21.01.11 odbyło się spotkanie Komitetu Klimatycznego Komisji UE, podczas którego radzono nad tym, jakie działania należy podjąć, aby zapewnić jak najbardziej jednolite i rygorystyczne standardy dotyczące bezpieczeństwa.

Pierwsza przymusowa przerwa w historii europejskiego handlu emisjami zostanie po stronie rejestrów krajowych wykorzystana nie tylko do tego, aby zainstalować lepsze systemy zabezpieczeń, jeśli w wielu małych rejestrach jest to w ogóle możliwe. O wiele bardziej wykorzystana zostanie ona do tego, aby przeprowadzić inwentaryzację oraz poddać kontroli każdy, fizycznie posiadany certyfikat. Oznacza to duże nakłady. Niezależnie od trudnej do oszacowania ilości ERU i CER trzeba będzie skontrolować 64- cyfrowe numery identyfikacyjne około 2,4 miliarda EUA. Suma ta wynika z jednorocznych, wydawanych w całej Europie podad 2 miliardów EUA oraz z pozostałego z lat ubiegłych, od roku 2008 nadmiaru, w wysokości ok. 400 milionów. Komisja będzie z pewnością chciała jak najszybciej zakończyć inwentaryzację, jako że już 1 marca kolejne 2 miliardy EUA zostaną wprowadzone na rynek.



Według wypowiedzi Dyrektora Generalnego UE Jos Debelke, poszukiwane są obecnie 2 miliony certyfikatów EUA pochodzących z ataków przeprowadzonych w ciągu ostatnich kilku dni, o wartości rynkowej 28,7 milionów Euro.

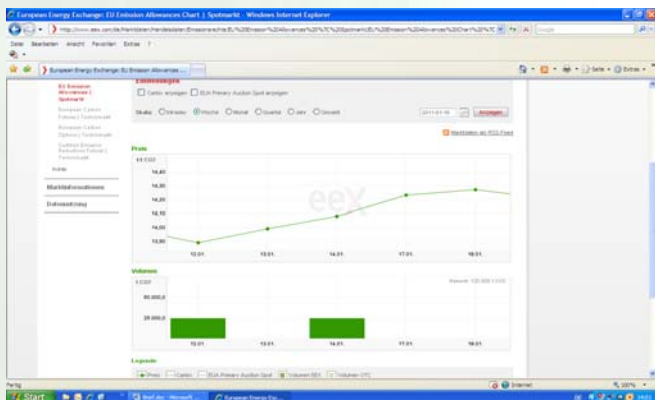
Kto jeśli potrafi liczyć oraz kieruje się zdrowym rozsądkiem zauważy, że w tej wypowiedzi rachunek nie uwzględnił 1,6 miliona certyfikatów pochodzących z Holcimia i że najprawdopodobniej nie zostały one w kalkulowane, jako że straty te powstały już w listopadzie 2010 roku.

Jeśli dodamy 475.000 certyfikatów Blackstone oraz 488.000 certyfikatów z rezerw austriackich, do 2 milionów skradzionych certyfikatów o których zakomunikowano brakuje jeszcze 1.037.000 EUA, które musiały zostać w inny sposób utracone.

**Umacnia to teorię, że znacznie więcej, jak tylko jedno konto rejestrowe (Blackstone) w ciągu ostatnich dni zostało splądrowane.**

### Wpływ na giełdy CO2 oraz rynek handlowy

Giełdom Spot w Europie, w związku z decyzją o wstrzymaniu handlu, zalecano również wstrzymanie działań, co oprócz EEX w Lipsku, stało się o godzinie 17.00



*Handel EEX otwarty, lecz z powodu braku zaufania brak obrotów*

Handel terminowy certyfikatami CO2 nie został tą decyzją dotknięty, jednak w krótkim czasie załamał się do połowy swojego zasięgu, jako że informatyczno-techniczne zaniechanie się handlu Spot i Future w systemach giełdowych prowadzi do powstania poważnych problemów.

Ponieważ jednym z generalnych problemów konstrukcji ITS jest fakt, że prawo krajowe koliduje z (całkowicie rozsądnym) wyobrażeniem odnośnie organizacji i bezpieczeństwa Komisji UE, nie jest na przykład możliwe, aby lista skradzionych certyfikatów została

przez Komisję opublikowana. W zwiątku z tym każda giełda spot w Europie musi i chce zainstalować system kontroli wpływających certyfikatów CO2, który porównywalny jest do filtra by rozpoznawać zdefiniowane zakresy numerów certyfikatów. Wymaga to co nieco pracy, przy czym oczywiście spełniony musi być warunek, że giełda znajdująca się będzie w posiadaniu odpowiednich wykazów. Z prawnego punktu widzenia kłopoty są już zaprogramowane, jako że oficjalnie nie istnieją listy skradzionych certyfikatów, ponieważ odpowiednie prawo krajowe może być temu przeciwne.

Jeśli więc certyfikaty zostaną zablokowane do obrotu na giełdzie, lecz prawnie nie zostały one skradzione, może to w pojedynczych przypadkach prowadzić do wymagania wypłacenia odszkodowania.

Niezależnie od interesów giełd spot oraz konieczności większego zabezpieczenia systemu, interesujące jest, że głosy domagające się wstrzymania handlu spot na kilka miesięcy lub też jego całkowitego zlikwidowania, są coraz głośniejsze.

Kto na prawdę zna położenie wielu małych i średnich operatorów w UE, nie może tych głosów popierać.

Przez wszystkich oczekiwane zaniechanie się ochrony Środowiska oraz interesów gospodarczych zaszło tak daleko, że np. dla coraz większej ilości operatorów (przede wszystkim w Europie Wschodniej i Południowej), na porządku dziennym jest przeprowadzanie transakcji sprzedaży oraz ponownego odkupowania certyfikatów EUA, które umożliwiają szybkie osiągnięcie płynności finansowej. Poza tym, poprzez kryzys gospodarczy stało się jasnym, że zbyt silna regulacja rynku terminowego, której odpowiednio wcześniej nie zostanie przeciwstawiony zasób innych fizycznych rzeczy w formie towaru, złota, pieniędzy lub praw, prowadzić może do wielu poważnych problemów.

### Przegląd historycznych 18 miesięcy działalności przestępczej w EU- ETS

Krótkie spojrzenie na wydarzenia ostatnich 18 miesięcy w europejskim handlu emisjami pozwala na wyciągnięcie wniosków odnośnie powstałych potrzeb działania na poziomie Komisji UE oraz rejestrów krajowych.

- a) **07-2009** - zakrojone na dużą skalę, przeprowadzane przez bandy kryminalne oszustwo w zakresie podatku VAT w handlu prawami do emisji, zostaje w wielu krajach UE wykryte. Powstałe do tego momentu straty zostały oszacowane na 5 miliardów Euro



- b) **12-2009** - większa ilość osób została zatrzymana w związku z oszustwami podatkowymi, konta zostały zamrożone
- c) **01-2010** - w Belgii zatrzymane zostały kolejne 4 osoby podejrzane o oszustwa w handlu prawami do emisji, kradzież, paserstwo, oszustwa podatkowe związane z podatkiem VAT, etc.
- d) **02-2010** - oszuści internetowi kradną z kont rejestrowych w całej Europie, za pomocą ataku „Phishing”, certyfikaty o wartości milionów Euro. W związku z tym wysłane zostały wiadomości mailowe do wszystkich posiadaczy kont, co do których odbiorca zakładał, że wiadomości pochodzą z jego rejestru
- e) **02-2010** - w Norwegii, z powodu oszustw oraz nadużyć podatkowych związanych z certyfikatami CO<sub>2</sub>, ujęte zostały 3 osoby
- f) **03-2010** - rząd Węgier za pośrednictwem handlowca wprowadza do obiegu certyfikaty CER, które utraciły swoją ważność, jako że uprzednio zostały one wykorzystane do wypełnienia obowiązku umorzenia. Te nieważne certyfikaty doprowadziły do czasowego wstrzymania handlu emisjami na giełdzie
- g) **03-2010** - w Hiszpanii zostało aresztowanych 9 osób zamieszanych w oszustwa podatkowe w zakresie podatku VAT związanego z handlem emisjami. W Norwegii przebadane zostały wszystkie dotychczasowe transakcje wszystkich przedsiębiorstw
- h) **04-2010** - w Niemczech i Wielkiej Brytanii przeszukanych zostało 50 przedsiębiorstw, a 25 osób zostało aresztowanych w związku z podejrzeniem o oszustwa podatkowe związane z certyfikatami
- i) **05-2010** - po zakończeniu dochodzenia oraz dokonaniu oceny transakcji CO<sub>2</sub> przeprowadzonych w minionych miesiącach, dalsze zatrzymania w Norwegii
- j) **07-2010** - duży niemiecki bank zostaje przeszukany, przy czym cały dział handlowy certyfikatów CO<sub>2</sub> podejrzany jest o to, że wiedział o milionowych interesach związanych z nadużyciami w zakresie podatku VAT
- k) **08-2010** - czeski rejestr zastopował handel certyfikatami CO<sub>2</sub> z powodu większej ilości zdarzeń związanych z nadużyciami w zakresie podatku VAT popełnionych przez uczestników rynku
- l) **11-2010** - rumuńskiej cementowni Holcim, za pomocą wirusa komputerowego, skradziono z konta rejestrowego 1,6 miliona EUA o wartości 23 milionów Euro. Milion certyfikatów do tej pory nie został odnaleziony, 600.000 zamrożonych jest na różnych kontach
- m) **11-2010** - włoskie urzędy wstrzymują handel emisjami i przeszukują setki przedsiębiorstw z powodu podejrzenia o nadużycia w zakresie podatku VAT oraz o paserstwo, jako że certyfikaty kupowane były po cenie znacznie niższej od ceny rynkowej. Straty podatkowe oszacowano na 500 milionów Euro
- n) **01-2011** - z austriackiego rejestru, po ataku hakerów skradzione zostały krajowe rezerwy certyfikatów EUA, w wysokości 488.000
- o) **01-2011** - poprzez zagrożenie wybuchem bomby, splądrowany został rejestr czeski oraz poprzez działania hakerów skradzione zostały dane rejestrowe klientów- rozmiar kradzieży nie jest do tej pory znany
- p) **01-2011** - rejestry Polski i Estonii odwiedzone zostały przez hakerów, jednak (do tej pory) obie strony zaprzeczają dokonaniu kradzieży zarówno danych klientów, jak i certyfikatów
- q) **01-2011** - konto rejestrowe czeskiego usługodawcy w zakresie CO<sub>2</sub> Blackstone Global Venture zostało splądrowane przy wykorzystaniu skradzionych uprzednio z systemu rejestrowego danych dostępowych, skradzionych zostało 475.000 EUA- wśród skradzionych certyfikatów stwierdzono obecność 13.100 EUA, które już wcześniej zostały skradzione

### Rejestry krajowe częściowo z takimi standardami organizacyjnymi i zabezpieczeniami jak przed 200 laty?

Jeśli przyjrzeć się uprzedniej liście wydarzeń związanych z handlem emisjami w Europie, można odnieść wrażenie, że handel ten po części posiada stopień organizacyjny oraz poziom zabezpieczeń, jak przed 200 laty.

Szczególnie jako insider (ale również jako osoba postronna) od jakiegoś czasu postawić można sobie pytanie, jak to jest możliwe, że w handlu emisjami możliwe są wydarzenia, które w innych branżach byłyby niemożliwe do pomyślenia.

Jedną z takich, stosunkowo niewytłumaczalnych rzeczy jest na przykład pytanie, jak to jest możliwe, że w czasach wysoko zaawansowanej technologii informatycznej certyfikat CO<sub>2</sub> posiadający (analogicznie jak banknoty) jednoznaczny numer identyfikacyjny, oraz który na dodatek nie występuje w formie papierowej, a w obiegu znajduje się tylko jako



wirtualne, elektroniczne prawo, nie może zostać odnaleziony.

Laik mógłby sądzić, że elektroniczne prawo (certyfikat), można tak ukryć na koncie, że nie może on zostać odnaleziony. Dotyczyć by to mogło być może, w niektórych okolicznościach, nieoptymalnie prowadzonego konta w krajach rozwijających się na końcu świata i odnosić się do certyfikatów CER.

W przeciwieństwie do nich certyfikaty EUA nie mogą opuścić terenu UE, a w związku z tym również rejestru UE, czyli pozostają w Europie Centralnej.

Jeśli więc w „zamkniętym garnku” europejskich rejestrów CO<sub>2</sub>, które prowadzone są przez odpowiednie urzędy rządowe, w dowolnym momencie nie można szukać i znaleźć ponumerowanych elektronicznych certyfikatów, to jest to stan bardzo mizerny (zobacz infobox po prawej).

W dalszym ciągu zapytać można, dlaczego państwa członkowskie UE dopuszczają do miliardowych prawdopodobnie osiągających już wysokość do 10 miliardów Euro- oszustw podatkowych tylko dlatego, że nie są w stanie lub nie chcą wprowadzić we wszystkich krajach postępowania Reverse- Charge (obowiązek podatkowy odnośnie podatku VAT przechodzi na odbiorcę), które z pewnością byłoby barierą dla oszustw podatkowych.

Z punktu widzenia poszkodowanych właścicieli kont nasuwa się pytanie, dlaczego właściwie standardy bezpieczeństwa dla zarządzania kontami rejestrowymi CO<sub>2</sub> tak bardzo odbiegają od tych, jakie dotyczą kont bankowych. Ma się wrażenie, a następnie bardzo szybko pewność, że handel emisjami jest w stosunku do porównywalnych zastosowań opóźniony w rozwoju o 10 lat.

Przyznać jednak należy, że niektóre z wielu problemów spowodowane są tym, że

- prawa krajowe poszczególnych państw członkowskich przeciwne są wprowadzeniu jednolitego sposobu prowadzenia kont na poziomie UE
- państwo, które dopiero niedawno przystąpiło do UE prawie nie posiada doświadczenia dotyczącego prowadzenia konta
- niektórzy z prowadzących konta mogą/chcą być mądrzy dopiero po szkodziu
- różnorodne wersje oprogramowania rejestrów krajowych nie mogą być w porównywalny sposób wyposażone

Jedno jest całkowicie jasne:

Aby handlu emisjami nie trzeba było szybko i ostatecznie uznać za niepowodzenie, państwa oraz ich

rejestry, które nie są odpowiednio wyposażone nie powinny mieć prawa do udziału w handlu, powinny prosto zostać z niego wyłączone do momentu, aż nie zostanie osiągnięty odpowiedni poziom organizacyjny oraz w zakresie bezpieczeństwa.

Włamywacz będzie zawsze wchodził do domu, do którego wnętrza najprościej jest się dostać, aby osiągnąć swój łup.

### Infobox

#### ***Ironiczne porównanie sytuacji takich jak na Dzikim Zachodzie***

*Na Dzikim Zachodzie Ameryki dokonywano z wielką regularnością napadów na banki oraz pocztylionów, okradano klientów i zabierano wynagrodzenia. Jeśli szeryf i jego ludzie próbowali pomóc poszkodowanemu w złapaniu bandyty, ten często przekraczał granicę, gdzie nie sięgała już jurysdykcja lokalnego obrońcy prawa. Pozostawali wtedy- obok jednego, czy drugiego zmarłego jeźdźca- również poszkodowani klienci, którzy z powodu braku lub niewystarczającego ubezpieczenia musieli w jakiś sposób wyrównać stratę finansową. Również już wtedy dochodziło do tego, że ilość bandytów w niektórych rejonach tak zwiększała swoją ilość, że w końcu musieli oni, z powodu braku potencjalnych ofiar, napadać na siebie wzajemnie.*

Równolegle Komisja powinna się zastanowić, czy rzeczywiście każdy ma prawo do otwarcia konta rejestrowego, aby zawodowo handlować certyfikatami.

Oczywistym jest, że od 24 miesięcy duża ilość osób otwiera konta wyłącznie po to, aby handlować certyfikatami, **choć z gospodarczego punktu widzenia nie powinno to być dopuszczalne!**

Mówiąc inaczej: od momentu wprowadzenia handlu emisjami w roku 2005 każdy znany na rynku handlowiec (jak np. Emissionshändler.com) ma swoich klientów. Ilość klientów w Europie jest ograniczona i prawie nie rośnie lub nawet zaczyna spadać (wystąpienie małych emitentów). Od czasu do czasu klient przechodzi od jednego handlowca do drugiego, tak jak to reguluje rynek oraz zasady konkurencji).

**Równolegle do tego ilość „handlowców” wzrosła prawie stukrotnie.**

W Niemczech na równo 2.000 kont operatorów przypada w chwili obecnej około 540 kont handlowców ( w początkach handlu CO<sub>2</sub> było ich mniej, niż 100). Obecnie **udział handlowców stanowi równo 27%.**



W krajach, gdzie wydanie zezwolenia na prowadzenie handlu emisjami nie przebiega tak poprawnie, jak w Niemczech, liczby te są o wiele wyższe. I tak przypada

- W Rumunii na 270 operatorów 90 handlowców = **33%**
- W Czechach na 430 operatorów 190 handlowców = **44%**
- W Estonii na 60 operatorów 40 handlowców = **150%**
- W Danii na 410 operatorów 1.340 handlowców = **319%**
- W Lichtensztajnie na dwóch operwtorów 200 handlowców= **5.000%**

Jeśli przyjrzeć się w rejestrze UE fantastycznym nazwom przedsiębiorstw oraz ich stronom internetowym (które w wielu przypadkach w ogóle nie istnieją), szybko stanie się jasnym, co od dwóch lat dzieje się w europejskim handlu emisjami. Dla wtajemniczonych jest to już od dawna jasne. Przypuszczenie to, na podstawie ostatnich wydarzeń, zostało również wypowiedziane przez stronę oficjalną:

**„EU officials could not rule out the possibility that regular traders had perpetrated the theft”**

(Źródło: doniesienie Reutera z 20.01.11)

Uprzednie, ostrożne sformułowanie można nieco dosadniej przetłumaczyć jako:

**„ Możliwym/prawdopodobnym jest, że kradzieże popełnione zostały przez zwyczajnych handlowców”**

### Disclaimer

GEMB mbH nie ponosi ani wyraźnej, ani milczącej odpowiedzialności za dokładność oraz kompletność zamieszczonych informacji, jak również ich przydatności do konkretnych celów.

List dotyczący emisji wydany jest na stronie [www.handel-emisjami.pl](http://www.handel-emisjami.pl) przez GEMB mbH i służy wyłącznie celom informacyjnym. Informacje w nim zawarte nie podlegają gwarancji ze względu na ich dokładność oraz kompletność. Decyzje kupna lub sprzedaży podjęte na podstawie zawartych w liście informacji zawarte są przez przedsiębiorcę dobrowolnie oraz bez oddziaływania osób trzecich.

### Emissionshändler.com<sup>®</sup>

Członek Austriackiej Giełdy Energetycznej EXAA  
częściowy udziałowiec APX(Amsterdam Power Exchange)  
z EEX Leipzig (European Energy Exchange)  
z Zarządem Niemieckiego Związku Handlu Emisjami  
i Ochrony Klimatu [www.bvek.de](http://www.bvek.de)  
GEMB mbH, Helmholtzstraße 2-9, Niemcy -10587 Berlin  
Telefon: +49 30 – 897 25 954, Telefon: +49 30 – 398 8721-31  
Telefax: +49 30 – 398 8721-29  
Web: [www.emissionshaendler.com](http://www.emissionshaendler.com) , [www.handel-emisjami.pl](http://www.handel-emisjami.pl)  
Mail: [nielepiec@handel-emisjami.pl](mailto:nielepiec@handel-emisjami.pl) , [info@emissionshaendler.com](mailto:info@emissionshaendler.com)