Událost ze dne 18. ledna 2011 v českém Rejstříku obchodování s povolenkami na emise skleníkových plynů

Závěrečná zpráva o výsledcích interního šetření

Obsah:

1. Popis události

Dne 18. ledna 2011 v čase mezi 9:00 a 16:00 hodinou bylo iniciováno a dokončeno pět problematických transakcí v českém Rejstříku obchodování s povolenkami na emise skleníkových plynů.

Později byly přijaty reklamace na tři z těchto transakcí se zdůvodněním, že transakce byly iniciovány bez vědomí držitelů účtů. Ve všech třech případech se jednalo o odchozí transakce na účet v jiné zemi. Dvě z nich směřovaly do Polska a jedna do Itálie. Celkový objem těchto tří transakcí byl 1,175 miliónů povolenek.

Kromě těchto 3 transakcí byly také dne 18. ledna 2011 iniciovány a dokončeny dvě jiné problematické transakce. Jedna transakce byla vnitrostátní v objemu 31 000 povolenek. Všechny okolnosti kolem této transakce jsou podobné jako tři předchozí transakce, ale dosud jsme neobdrželi žádnou stížnost na tuto transakci. Správce rejstříku kontaktoval držitele účtů, avšak bez odezvy.

Poslední problematická transakce ze dne 18. ledna 2011 je odchozí mezinárodní transakce v objemu 100 000 povolenek. Držitel účtu, který inicioval tuto transakci, figuruje také v předchozí problematické transakci. Sériová čísla povolenek z této transakce jsou na seznamu ukradených povolenek z řeckého rejstříku.

Přehled problematických transakcí:

Druh transakce	**Držitel účtu**	**Počet transakcí**	**Počet povolenek**
Nelegální transakce – obdrželi jsme stížnost od držitele účtu	Odchozí - mezinárodní	3	1 175 000
Podezřelá transakce	Vnitrostátní	1	31 000
Podezřelá transakce	Odchozí - mezinárodní	1	100 000
Celkem		**5**	**1 306 000**

2. Provedená okamžitá opatření dne 19. ledna 2011

Provedená opatření dne 19. ledna 2011 jsou uvedena v následujícím přehledu:

Čas	Popis
7:56	První reklamace držitele účtu na provedenou transakci dne 18. ledna 2011.
8:35	Po kontrole této transakce a revizi kmenových dat držitele účtů v databázi rejstříku český správce (OTE) rozhodl provést bezpečnostní odpojení rejstříku podle pravidel Sekretariátu Rámcové úmluvy OSN o změnách klimatu.
8:39	Český správce (OTE) požádal svého provozovatele IT infrastruktury (Logica) o uzavření českého rejstříku pro všechny externí uživatele.
8:48	Český správce (OTE) informoval ITL (Nezávislá evidence transakcí, ústřední místo registrovaných transakcí v rámci Kjótského protokolu – spadá pod INFCC) o porušení bezpečnosti a požádal ITL o zastavení provozu českého rejstříku.
9:08	IT provozovatel informoval OTE o uzavření systému pro všechny externí uživatele (web server nebyl přístupný pro externí uživatele).
9:37	Český správce rejstříku (OTE) informoval CITL (nezávislá evidence transakcí Společenství; ústřední místo registrovaných transakcí v rámci EU ETS – spadá pod EK) informoval o: • Narušení bezpečnosti českého rejstříku, • Uzavření českého rejstříku, • Žádost do ITL o převedení českého rejstříku do stavu „Not Operating“.

3. Vyšetřování incidentu

Útok na český registr byl veden neznámým agresorem, využívajícím přihlašovací údaje jednoho z administrátorů rejstříku (přihlašovací jméno a heslo). Přihlašovací údaje administrátora nebyly vědomě nikomu vyzrazeny.

V počítači tohoto administrátora byl nalezen Trojský kůň a po odhalení byl z počítače okamžitě odstraněn. Standardní antivirový program tento virus neodhalil. Vyšetřování orgány Policie vychází také z předpokladu, že tento virus Trojský kůň skenoval přihlašovací jména a hesla všech aplikací, užívaných administrátorem

rejstříku. Touto cestou mohly být vyzrazeny přihlašovací údaje pro aplikační software Seringas, který podporuje infrastrukturu rejstříku účtů.

Agresor se přihlásil do rejstříku jako administrátor dne 18. ledna 2011 v 0:09 hod středoevropského času. Změnil hesla několika zmocněných zástupců majitelů účtů a modifikoval jejich kmenová data. Potom se přihlásil do rejstříku skrze přístupy několika zmocněných zástupců a inicioval 3 nebo 4 transakce.

Z analýzy provozu je zřejmé, že poslední aktivita v rejstříku proběhla dne 18. ledna 2011 v 15:13 hodin středoevropského času.

OTE, jako správce rejstříku, zaznamenal několik nedůvěryhodných e-mailů. Souvislost mezi těmito e-maily a útokem je předmětem vyšetřování Policie ČR.

S neoprávněným přístupem k počítačovému systému OTE spojujeme i evakuaci budovy, v níž OTE sídlí dne 18. ledna 2011 v 12:10 hodin. Následující den bylo objasněno, že důvodem této evakuace byla pohrůžka bombového útoku v poschodí OTE zaznamenaná telefonickým oznámením Policii.

Správce českého rejstříku se nacházel mimo budovu dne 18. ledna 2011 od 12:10 do 16:30 hodin. Informační systému rejstříku povolenek byl dostupný po celou tuto dobu.

4. Přijatá opatření pro zvýšení bezpečnosti

1. Během odstávky rejstříku správce rejstříku zahájil řádně plánovaný a ohlášený upgrade rejstříku. Systém byl kompletně zálohován (hardware, software, databáze) a nový hardware a software je připraven.
2. S opětovným otevřením rejstříku bude vyžadován druhý faktor pro autorizaci koncového uživatele (heslo zasílané SMS).
3. „IP tracking modul“ pro přihlašování uživatele do systému a provádění transakcí je v nové verzi rovněž připraven.
4. Jakmile v českém rejstříku bude stav „Not Operating“ změněn na „Reconciliation only“, správce českého rejstříku může:

- dokončit upgrade,
- obnovit všechna kmenová data držitelů účtů a zmocněných zástupců, změněná agresorem účtů během incidentu.

5. Na základě požadavků zaslaných Evropskou komisí bude zpracován nezávislý posudek logů a penetračních testů. Zpráva bude doručena Evropské komisi.
6. Všichni administrátoři rejstříku změní svá hesla pro přístup do rejstříku.
7. Hesla pro přístup do lokální sítě e-mail (LAN) a server společností OTE byla změněna pro všechny zaměstnance.
8. Zaměstnancům byla upravena administrativní práva na koncových stanicích.