MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Situační zpráva
o vybraných oblastech bezpečnosti

energetická bezpečnost, bezpečnost finančních institucí,
informační technologie a kybernetická bezpečnost, krizové řízení

za období 1. července do 31. prosince 2014

Odbor bezpečnostní politiky Ministerstva vnitra

březen 2015

OBSAH

ÚVODEM

Vážení čtenáři,

dostává se Vám do rukou periodická situační zpráva, která mapuje vybrané oblasti bezpečnosti v druhé polovině roku 2014 (řada statistik nicméně pro přehlednost obsahuje shrnutí za celý rok). Těmito vybranými oblastmi jsou: energetická bezpečnost, bezpečnost finančních institucí, kybernetická bezpečnost a informační kriminalita a krizové řízení. Tuto zprávu zpracovává odbor bezpečnostní politiky Ministerstva vnitra.

Potřeba vzniku tohoto materiálu vyplynula z diskuse Ministerstva vnitra s některými soukromými subjekty, které o takový výstup projevily zájem. Sledovat tato odvětví bezpečnosti doporučila České republice i Evropská unie. Každá z vybraných oblastí má totiž nemalou důležitost pro zajištění celkové bezpečnosti ČR, nicméně žádná ze státních institucí se dosud jejich periodické analýze z pohledu bezpečnosti systematicky nevěnovala. Tato zpráva se snaží tuto mezeru alespoň částečně zaplnit. Je určena jak všem zástupcům soukromých subjektů, působícím v některém ze zmíněných odvětví, tak i všem zájemcům o bezpečnostní problematiku jako takovou.

Každé výše uvedené oblasti je věnována samostatná kapitola, která vždy obsahuje výběr nejdůležitějších událostí, k nimž ve sledovaném období došlo (se stručným popisem každé z nich) a dále statistická data, týkající se především kriminality a mimořádných událostí v probíraném sektoru. Zdrojem těchto údajů jsou zejména Policie České republiky a Hasičský záchranný sbor. Kromě samotných tabulek a čísel nechybí v této části ani určitá interpretace a analýza hlavních trendů současnosti, včetně výhledů do budoucna.

Některé kapitoly jsou rozšířeny o podrobnější analýzu souvisejících fenoménů. V případě kybernetické bezpečnosti je tak zvláštní oddíl věnován rizikům technologií Smart Homes. V sekci o energetické bezpečnosti čtenář nalezne analýzu příčin a dopadů dramatického poklesu cen ropy, kapitola zaměřená na krizové řízení podrobněji informuje o mimořádné události v muničním areálu ve Vrběticích. Stejná kapitola je dále rozšířena o přehled připravovaných velkých cvičení v roce 2015.

Poslední dvě části zprávy jsou pro všechny čtyři zkoumané oblasti společné. První z nich se věnuje legislativním změnám, ke kterým v každém odvětví ve sledovaném období došlo, druhá pak shrnuje nadcházející setkání a konference, které budou věnovány bezpečnostním otázkám, a účast na nich by tak mohla být přínosem jak pro zmíněné pracovníky soukromých firem, tak pro další zájemce o danou problematiku.

Zprávu pochopitelně není nutné číst celou od začátku do konce; lze předpokládat, že každý čtenář se zaměří především na tu část, která je předmětem jeho profesního či soukromého zájmu. Je nicméně nutné v této souvislosti upozornit, že některé kapitoly se částečně obsahově prolínají (např. bezpečnost finančních institucí a informační kriminalita, či energetická bezpečnost a krizové řízení). V závěru pak naleznete seznam zdrojů použitých pro vypracování této zprávy.

RESUMÉ

První kapitola této zprávy je věnována údajům o celkové kriminalitě v České republice v roce 2014. Policejní statistiky v této oblasti odhalují velmi pozitivní trend pokračujícího poklesu celkového počtu trestných činů, který započal již v roce 2010 (s krátkým přerušením v roce 2013). Celková kriminalita za rok 2014 byla dokonce nejnižší za posledních 10 let, stejné je to i v součtu celkových škod.

K meziročnímu poklesu došlo v roce 2014 u všech základních druhů kriminality, kromě mravnostní a hospodářské. Pokles byl zaznamenán ve všech krajích, vůbec největší byl v Praze, ve středních Čechách, ale také na severní Moravě. Vzrostla také míra objasněnosti trestné činnosti na celkových 49 %.

Konkrétnější data je možné nalézt v následujících kapitolách, věnovaných jednotlivým oblastem bezpečnosti. Kapitola o energetické bezpečnosti nabízí statistické údaje Hasičského záchranného sboru a Policie České republiky ve vztahu k objektům energetické infrastruktury. Podrobnější analýza je pak věnována dramatickému pádu cen ropy a jeho důsledkům v globálním i českém měřítku. Zvláštní oddíl je pak věnován cvičení DRILL 2014.

Kapitola o bezpečnosti finančních institucí v sekci věnované policejním statistikám upozorňuje na výrazný pokles počtu loupežných přepadení finančních institucí, který se, doufejme, stává počátkem nového trendu. Počet těchto skutků poklesl meziročně téměř o polovinu. Internacionální charakter organizovaných balkánských skupin, věnujících se skimmingu a zneužívání kreditních karet, dokládají popsané případy mezinárodní policejní spolupráce za asistence Europolu. Speciální oddíl je pak věnován novým trendům v autorizaci on-line finančních transakcí, zejména pak nejnovějším možnostem v oblasti biometrie a behaviometriky.

Další část zprávy se zabývá kybernetickou bezpečností a informační kriminalitou. Ta je jednou z nejrychleji se rozvíjejících forem kriminality – také v tomto roce zaznamenaly policejní statistiky nárůst trestné činnosti, páchané s pomocí výpočetní techniky, o téměř 40%. Tento trend trvá bez přestávky již mnoho let a bohužel se, vzhledem k pokračujícímu pronikání informačních technologií do dalších oblastí života společnosti, nedá očekávat jeho brzký zvrat. V tradiční sekci věnované novinkám od bezpečnostních složek a státní správy jsou blíže popsány aktivity klíčových státních institucí, tedy zejména Policie ČR (informační kriminalita) a Národního bezpečnostního úřadu (kybernetická bezpečnost). Delší analýza je věnována novému fenoménu technologií Smart Homes, především jejich možným rizikům.

Podstatná část kapitoly o krizovém řízení je věnována statistikám Hasičského záchranného sboru a jeho evidenci mimořádných událostí za rok 2014 (rozsáhlejší verzi těchto podkladů naleznete přímo na stránkách www.hzscr.cz). Obsažen je přehled největších požárů uplynulého roku a velkých cvičení, která jsou v budoucnu plánována. Delší exkurz je věnován mimořádné události v muničním areálu Vrbětice a tragické události ve Žďáře nad Sázavou.

Poslední dva oddíly zprávy poukazují na některé legislativní změny, které ve zkoumaných oblastech proběhly a rovněž zde naleznete odkazy na řadu konferencí a akcí věnovaných bezpečnosti zmiňovaných sektorů.

CELKOVÁ KRIMINALITA V ČR V ROCE 2013

Registrovaná kriminalita v meziročním srovnání[1]

Za období od 1. 1. do 31. 12. 2014 Policie ČR registrovala **celkem 288 660 trestných činů**, což představuje **poměrně výrazný meziroční pokles** (-36 706, -11,3 %). Znamená to tedy definitivní návrat k trendu poklesu celkové kriminality, započatému rokem 2010, který byl jen dočasně přerušen v roce 2013 (což bylo dáno zřejmě celkovou hospodářskou situací v zemi, která má na objem celkové kriminality zásadní vliv). Celková **kriminalita za rok 2014 byla dokonce nejnižší za posledních 10 let**.

Kriminalita klesala ve všech oblastech České republiky. **Největší pokles byl registrován v Praze** (-10 177, -12,4%), Středočeském kraji (-6 232, -16,7 %) a Moravskoslezském kraji (-5 620, -13,1 %). **Nejmenší pokles byl zaznamenán v Jihočeském kraji** (-337, -2,2 %).

K meziročnímu poklesu došlo v roce 2014 u všech základních druhů kriminality, kromě mravnostní a hospodářské:

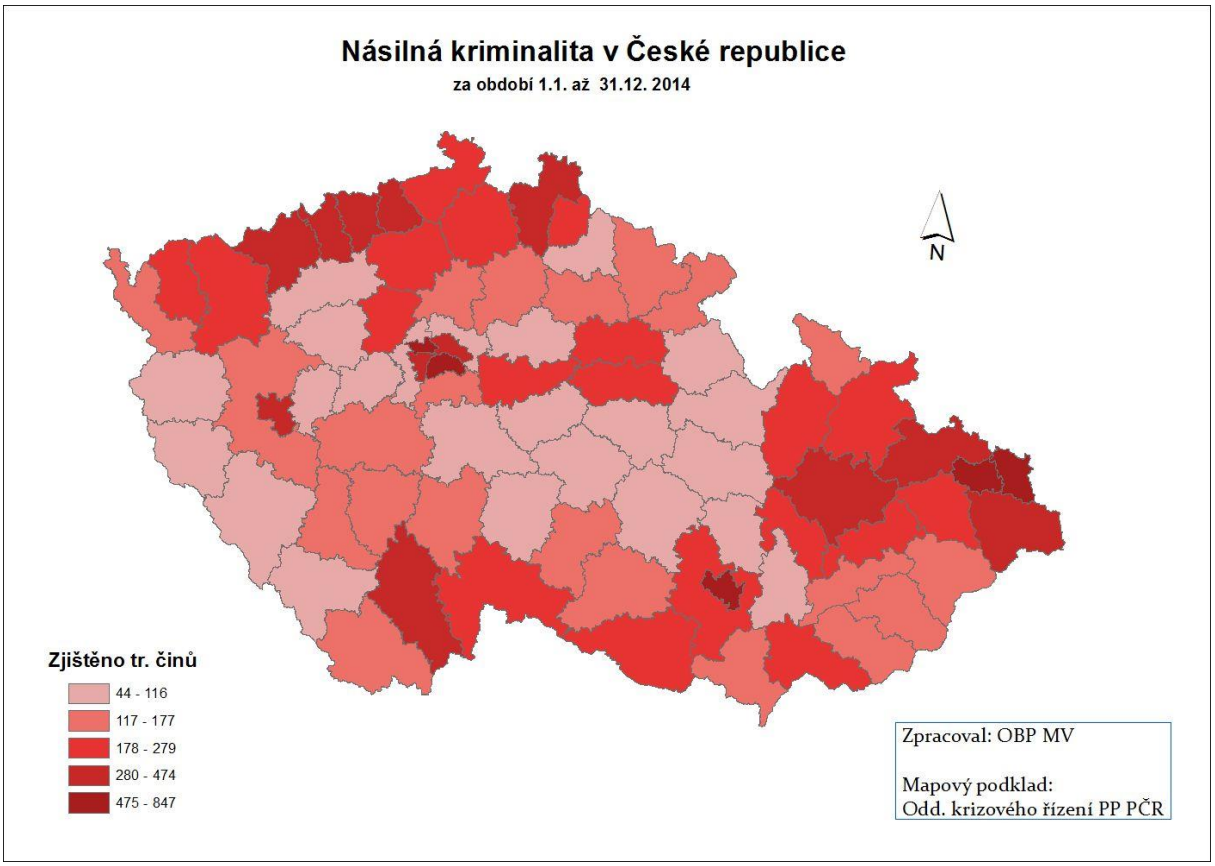
- násilná kriminalita (-6,5 %); celkem zjištěno 16 949 skutků, objasněno 70,3 % z nich; klesl i počet vražd na 160 skutků (objasněnost 91,3 %)
- mravnostní kriminalita (+4,6 %), celkem 2 205 skutků, objasněnost 70,4 %; vzrostl především počet znásilnění (o 80 více skutků než v roce 2013, což je nárůst o 13,6 %)
- majetková kriminalita (-17,1 %), celkem 173 611 skutků, objasněnost 23,6 %; došlo k plošnému poklesu takřka u všech druhů krádeží prostých (jako jsou kapesní krádeže, krádeže jízdních kol či krádeže v bytech), ale i u krádeží vloupáním. Po roce 2013 se obnovil dlouhodobý pokles tzv. autokriminality (krádeže motorových vozidel, věcí z aut, součástek motorových vozidel)
- hospodářská kriminalita (+1,2 %), celkem 30 731 skutků, objasněnost 55,1 %; hospodářská kriminalita má nejvyšší podíl na celkových škodách (72,7 %), nejvyšší podíl má trestný čin krácení daně se zjištěnou škodou přes 8,5 miliardy Kč

Vzrostla také celková míra objasněnosti, meziročně o 5,3 % na 49%. Pozitivní je i **pokles zjištěných škod o 1,2 %** na hodnotu 28,69 miliard Kč. Z hlediska dlouhodobého vývoje registrovaná kriminalita stagnuje, resp. postupně klesá. Značná část kriminality je řešena ve zkráceném přípravném řízení, na nějž navazuje zjednodušené řízení před samosoudcem, završené vydáním trestního příkazu. Zkrácené přípravné řízení se postupně stalo rozhodující formou přípravného řízení.

Policii ČR důvěřuje 65 % občanů, tedy nejvíce od roku 1993, jak vyplynulo z šetření Centra pro výzkum veřejného mínění ze září 2014.

[1] Detailní údaje o stavu kriminality zpracovává ÚSKPV PP PČR v pravidelné měsíční analýze „Aktuální stav kriminality v ČR ve statistikách“, kterou naleznete na intranetu na adrese: http://ppportal.pcr.cz/ntr/aktbs.htm. Nalézt je lze také v “Situační zprávě v oblasti vnitřní bezpečnosti”, kterou vydává odbor bezpečnostní politiky Ministerstva vnitra.

Ministerstvo vnitra reflektuje dlouhodobá i aktuální hlavní rizika a hrozby související s trestnou činností, jako jsou terorismus, organizovaný zločin, extremismus, korupce, závažná hospodářská kriminalita, informační kriminalita, drogová kriminalita atd. Zvláštní pozornost je věnována odčerpávání výnosů z trestné činnosti.



Stíhané a vyšetřované osoby

V roce 2014 bylo celkem **stíháno a vyšetřováno 114 611 osob**, což představuje meziroční pokles o 3 071 (-2,6 %). Značná je v tomto ohledu genderová nevyváženost, neboť 82 % stíhaných a vyšetřovaných byli muži. Odsouzeno bylo 72 823 osob.

Nejvíce pachatelů bylo stíháno a vyšetřováno pro krádeže prosté (20 014 osob) a zanedbání povinné výživy (12 494 osob), ohrožení pod vlivem návykové látky, opilství (10 399 osob), maření výkonu úředního rozhodnutí a vykázání (10 152 osob). Pachatelé těchto čtyř druhů trestných činů tvořili cca 46,3 % všech osob stíhaných a vyšetřovaných Policií ČR.

Počet dětí mladších 15 let, které byly vyšetřovány pro spáchání činů jinak trestných, se oproti loňské historicky nejnižší hodnotě zvýšil. Pokračoval ale pokles počtu stíhaných a vyšetřovaných mladistvých. Podíl recidivistů na celkovém počtu stíhaných a vyšetřovaných osob dlouhodobě stoupá a v roce 2014 dosáhl v historii ČR nejvyšší zaznamenané hodnoty 53,2 %. Z toho je patrná neúčinnost dosavadních opatření k předcházení recidivy trestné činnosti. Asi 6,4 % trestných činů měli v roce 2014 na svědomí cizinci.

***Zdroje pro tuto kapitolu**: Policie ČR, OBP MV*

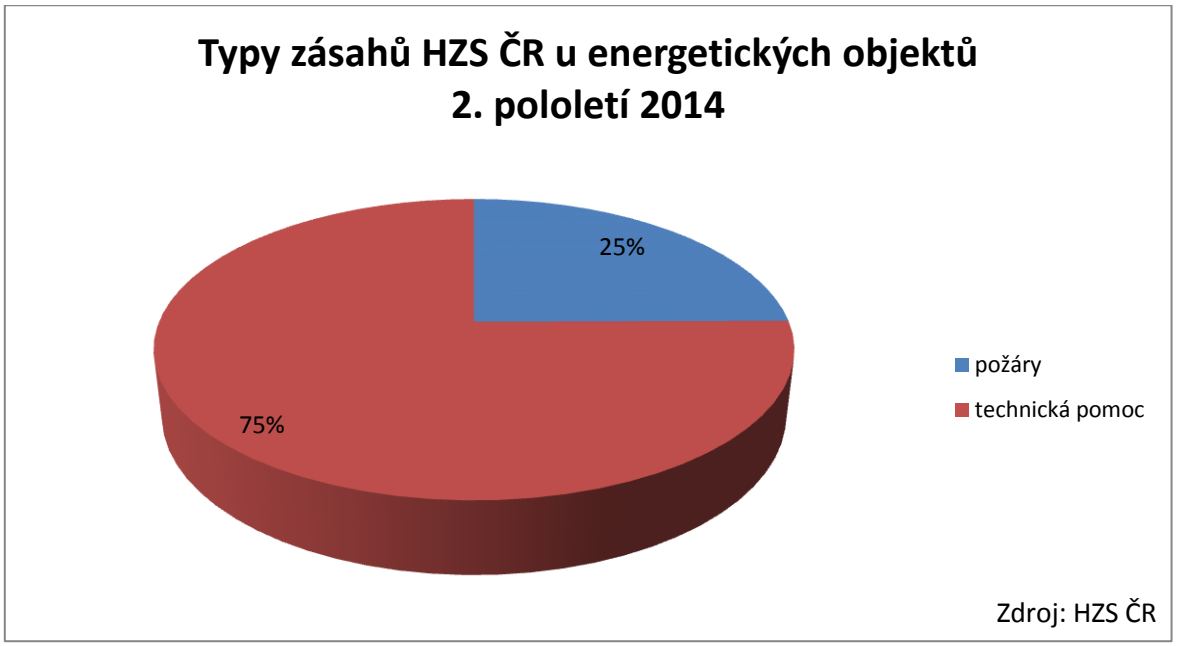
ENERGETICKÁ BEZPEČNOST

Hasičské statistiky a jejich interpretace

Ve druhém pololetí roku 2014 došlo oproti první polovině roku k poměrně výraznému poklesu počtu zásahů Hasičského záchranného sboru v energetických objektech (**pouze 249 případů oproti 494 případům z 1. pololetí, což je pokles o 50%**). Není zcela zřejmé, čím byl tento pokles způsoben, hlavní roli zřejmě hrály příznivější klimatické podmínky.

Vůbec nejhorším měsícem minulého roku z hlediska počtu zásahů byl totiž **květen (157 případů)** – tlaková níže Yvette tehdy přinesla do střední a jihovýchodní Evropy velké množství srážek. Nejhůře byly postiženy některé balkánské státy (velké povodně v Srbsku), také v ČR ale způsobily prudké deště a silný vítr značné potíže energetikům a zaměstnaly řadu jednotek HZS ČR. Hasiči pomáhali odstraňovat popadané stromy, které na mnoha místech poškodily elektrické vedení, velmi časté byly také výjezdy k čerpání vody ze zatopených energetických objektů. Komplikované povětrnostní podmínky přetrvávaly i počátkem června (113 případů). Naopak nejklidnějšími měsíci byly z hlediska počtu zásahů srpen a říjen (30 případů).

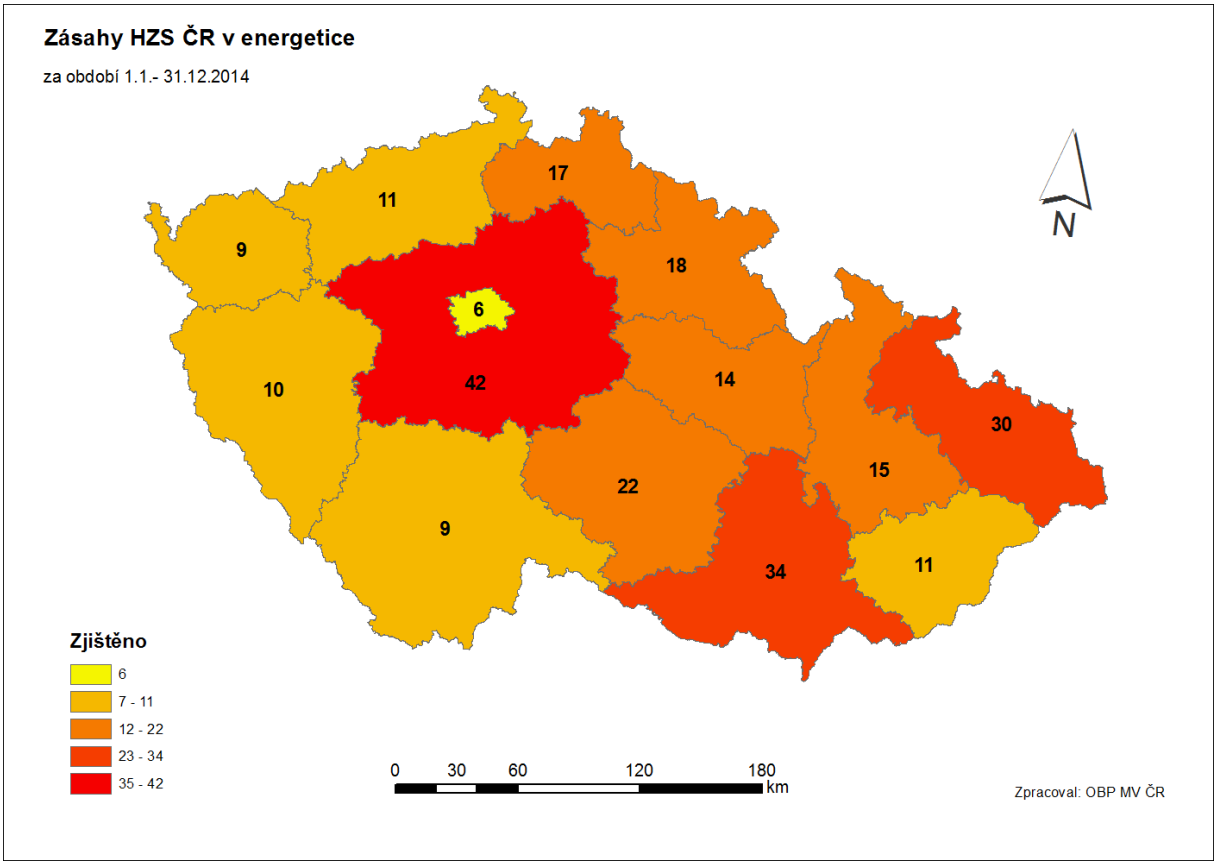
Úbytek bylo v 2. pololetí roku 2014 možné pozorovat hlavně v oblasti technických zásahů, neboť počet požárů v objektech energetické infrastruktury zůstal nezměněn (62 případů). V minulém pololetí tak výrazně **narostl podíl požárů na celkovém počtu zásahů** – ze 14 na 25 procent – jak znázorňuje také následující graf.



Pod širokou kategorií **technické pomoci** se skrývají např. pády stromů na elektrické vedení, čerpání vody z energetických zařízení při lokálních povodních a průtržích mračen, jiskřící kabely, měření koncentrace plynů a úniků různých nebezpečných látek, úniky páry atd. Může se ale také jednat o záchranu osoby na stožáru elektrického vedení, jako např. v prosinci 2014 v Mostě, kde se podle všeho jednalo o sebevražedný pokus, u kterého asistovala také státní a obecní policie a záchranná služba. Nejméně ve 14 případech vyjížděli ve sledovaném období hasiči ke zkratům v transformátorech, trafostanicích či v elektrickém vedení.

Stejně jako v předchozím pololetí nebylo ani v jednom případě nutné vyhlásit tzv. II. stupeň poplachu, který znamená zapojení velkého množství hasičských jednotek. Žádná z řešených událostí v energetické infrastruktuře tedy nepřerostla v havárii většího rozsahu.

Jak znázorňuje níže zobrazená mapa, ve druhé polovině roku 2014 došlo po několika letech ke změně na pozici kraje, který zaznamenal nejvyšší počet mimořádných událostí v energetické infrastruktuře. Tuto **nelichotivou první příčku držel dlouhou dobu se značným náskokem Moravskoslezský kraj, ten byl nicméně ve sledovaném období předstižen krajem Středočeským** (42 případů) a Jihomoravským (34 případů). Ve skutečnosti došlo ve všech krajích s výjimkou Karlovarského a Libereckého k poklesu počtu případů oproti 1. pololetí. Nejvýraznější byl pokles v kraji Olomouckém, kde bylo v první polovině roku zaznamenáno 62 případů, ve druhé pak pouhých 15. Nejméně výjezdů k energetickým objektům zaznamenali hasiči v hlavním městě Praze (pouze 6 případů, oproti 31 z 1. pololetí).



V roce 2014 hořelo přímo v energetických výrobních budovách v celkem 86 případech, což je o 12% méně, než v roce 2013. **Celková škoda z těchto událostí přesáhla 45,5 milionu Kč**, což je velmi výrazný pokles (o 76%) oproti roku 2013, kdy dosáhla výše 187 milionů Kč. V roce 2013 totiž došlo k několika mimořádně rozsáhlým událostem, o kterých jsme informovali v předchozích situačních zprávách. Dobrou zprávou rovněž je, že při těchto požárech nepřišel ve sledovaném období nikdo o život, zraněny byly celkem 3 osoby.

Pokud svůj pohled zaměříme na celé odvětví výroby a rozvodu elektřiny, plynu a vody, dosáhl počet požárů v roce 2014 hodnoty 157, což je o 13% méně než v roce 2013. Škoda dosáhla výše 37,7 milionu Kč, což představuje meziroční pokles o mimořádných 88%.

Naopak v odvětví těžby nerostných surovin, kde došlo v minulém roce 2014 k 14 požárům, škody v meziročním srovnání významně narostly, a to dokonce o 813% (jejich celková výše se vyšplhala na 53,1 milionu Kč). Stojí za tím zejména mimořádně rozsáhlý požár poháněcí stanice pásové dopravy firmy Severočeské doly a.s., se škodou 25 milionů Kč. K tomuto požáru došlo koncem března 2014 v obci Bílina-Břežánky v okrese Teplice.

Na závěr tradičně přehled velkých požárů (se škodou na 1 milion korun) druhé poloviny roku 2014 s dopadem na energetickou infrastrukturu:

Největší požáry související s energetikou v 2. pololetí roku 2014

16. 9. – **Požár pásového dopravníku**, důl Jiří, Vintířov, okr. Sokolov.
Příčina – v šetření.
Škoda – 2 500 000 Kč, požár likvidovaly 4 jednotky PO.

19. 12. – **Bioplynová stanice**, Dolní Lánov, okr. Trutnov.
Příčina: v šetření.
Škoda: 1 000 000 Kč, požár likvidovalo 6 jednotek PO.

Policejní statistiky a jejich interpretace

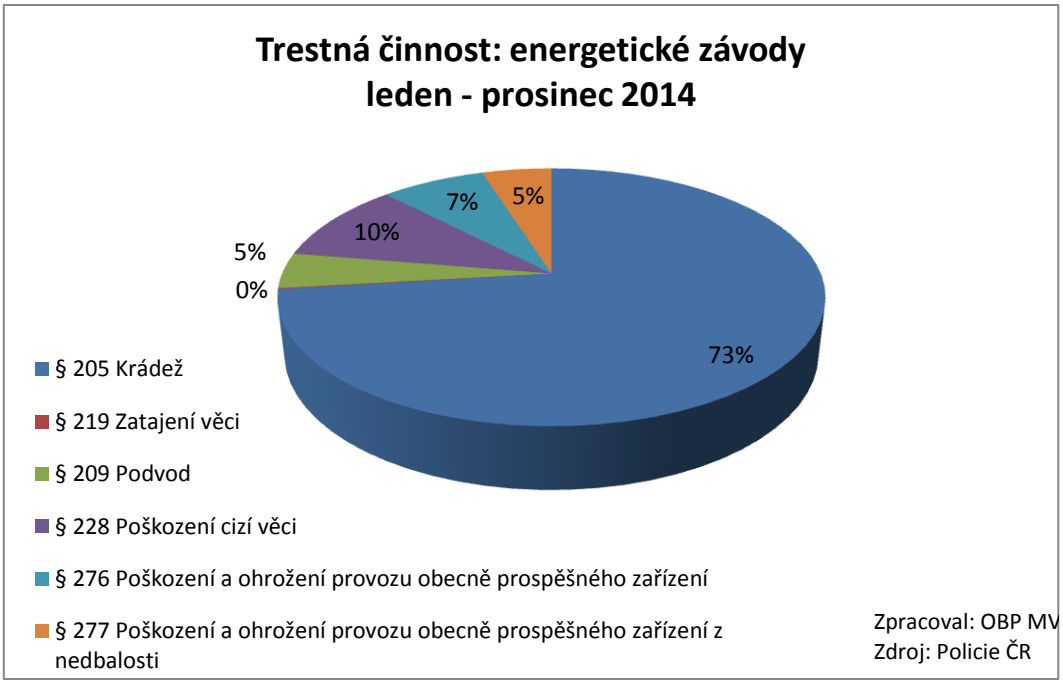
Co se týče trestných činů, souvisejících s elektrickou distribuční soustavou, jejich počet v meziročním srovnání mírně poklesl. V roce 2014 **policie zaznamenala 898 případů, kdy byly objektem napadení rozvody elektrického proudu nebo trafostanice**. Ve srovnání s rokem 2013 se jednalo o pokles o 18 % (tehdy bylo zaznamenáno 1087 případů). Pachatele se podařilo odhalit u 242 skutků, tedy ve 27 % případů. **Objasněnost tedy oproti roku 2013 stoupla o 8 %**. **Celkové škody dosáhly výše 66 558 800 Kč**, což je opět výrazně (téměř o polovinu) méně, než o rok dříve, kdy byly škody ve výši téměř 124 milionů. V meziročním srovnání tedy Policie ČR zaznamenala vesměs pozitivní trendy. V případě distribuční soustavy se **nejčastěji jedná o protiprávní čin krádeže** (§205, 618 případů), následované poškozením a ohrožením provozu obecně prospěšného zařízení (§276, 124 případů), poškozením cizí věci (§228, 107 případů), poškozením z nedbalosti (§277, 25 případů) a podvodem (§209, 24 případů).

V této oblasti lze také detekovat **velké regionální rozdíly**. **Elektrická rozvodná síť nejvíce trpí v důsledku krádeží v kraji Ústeckém (180 případů) a Moravskoslezském (119 případů)**, naopak nejlépe jsou na tom na Vysočině (pouhé 3 případy) a v Karlovarském kraji (9 případů). Nízký počet činů v Plzeňském (20) či Jihomoravském kraji (20) svědčí o tom, že počet případů není rozhodně dán jen velikostí či lidnatostí územního celku, ale svou roli zde hrají i jiné faktory (rozsah a dostupnost rozvodné sítě, sociální situace atd.). Zatímco v prvním pololetí dominoval policejním i hasičským (viz výše) statistikám poškozování energetické infrastruktury Moravskoslezský kraj, za celý rok 2014 byl v obou případech předstižen jinými regiony. Pokud se kromě rozvodné sítě zaměříme také na samotné **energetické závody**, evidovala PČR celkem 693 případů. Škody a objasněnost znázorňuje přehledně následující tabulka:

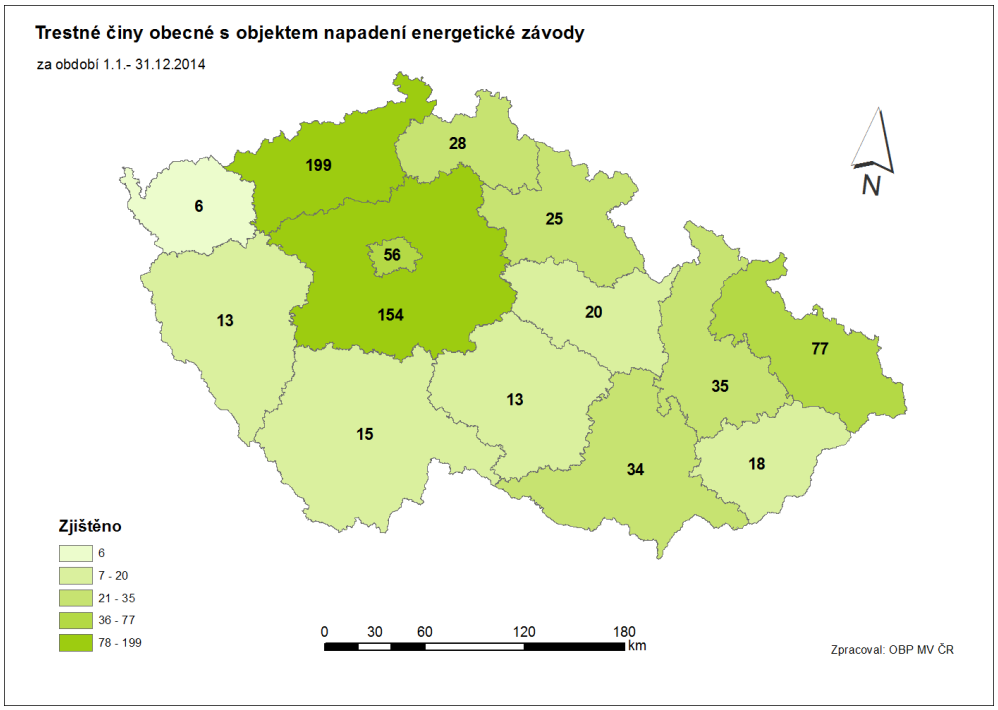
trestné činy, kde byly objektem napadení energetické závody za období leden až prosinec 2014

registrované skutky	693
počet skutků, u nichž byl zjištěn pachatel	247
škoda	62 145 000 Kč

Naprostá dominance krádeží je jasně patrná z následujícího grafu. Kradou se nejčastěji zpeněžitelné materiály – kabely, vodiče, elektroinstalační materiál, barevné kovy, oleje a pohonné hmoty. Započítány jsou ale také krádeže a ilegální odběry elektrické energie (135 případů). Je ovšem třeba připomenout, že trestná činnost v oblasti obecné kriminality generuje výrazně nižší škody, než kriminalita hospodářská. A tak třebaže prosté krádeže a krádeže vloupáním, tvoří téměř tři čtvrtiny všech skutků, na celkových zaznamenaných škodách mají méně než čtvrtinový podíl.



Geografické **rozložení protiprávní činnosti na energetických závodech** znázorňuje následující mapa. Patrná je zde **jednoznačná dominance Ústeckého (199 případů) a Středočeského kraje (154 případů)**, naopak nejméně postižen je v tomto ohledu kraj Karlovarský, což je dané nejen velikostí kraje, ale také rozmístěním jednotlivých prvků energetické infrastruktury.



Ze statistik také vyplývá, že v roce 2014 se staly v celkem 194 případech terčem trestného činu plynárny (zejména v Praze a na jižní Moravě), ve 49 případech elektrárny a v 87 případech teplárny (zejména v Ústeckém a Moravskoslezském kraji). Byly zaznamenány také 4 případy krádeže u objektů tranzitních ropovodů (s celkovou škodou 40 tisíc Kč), ke všem čtyřem pak došlo na Vysočině. Pachatele se podařilo dopadnout u tří z těchto čtyř případů. Tranzitní plynovody se staly v uplynulém roce terčem protiprávní činnosti pouze jednou, a to v Plzeňském kraji, přičemž se jednalo o nedbalostní poškození. Škoda při něm přesáhla 75 tisíc Kč.

Fenomén: pád cen ropy a jeho důsledky v globálním i českém měřítku

Americká břidlicová revoluce

V posledních několika letech dochází k **dramatickému nárůstu těžby ropy a zemního plynu z tzv. „nekonvenčních zdrojů“**. Nekonvenčních metod je celá řada, využitelné jsou například dehtové písky či biopaliva (získávání paliv z rostlin jako je řepka či cukrová třtina). Možná je také přeměna uhlí či zemního plynu na další uhlovodíková paliva; právě z uhlí získávalo za války nemalou část své ropy nacistické Německo, podobně také Jihoafrická republika v časech mezinárodní izolace, způsobené režimem apartheidu.

Jako nejperspektivnější se ale v současné době jeví **těžba ropy a zemního plynu z břidlicových hornin**. Břidlicové vrstvy totiž často obsahují množství usazených organických látek (tzv. kerogenu) – jedná se v podstatě o zbytky těl živočichů a rostlin, tedy základního materiálu pro vznik ropy i zemního plynu. Konvenční ropa také z kerogenu vzniká – obvykle se ale jedná o proces trvající stovky tisíc let a vyžadující dlouhodobé působení tlaku a tepla. Tento proces je nicméně možné chemicky urychlit (např. tzv. pyrolýzou, během které se ropné břidlice zahřívají na teploty kolem 500°C bez přístupu kyslíku). Podobné je to u břidlicového plynu, který se získává nejčastěji metodou hydraulického štěpení (tzv. frakování), kdy se v hornině vytvářejí umělé praskliny, které zajistí průchodnost plynu a jeho produkci v komerčním množství.

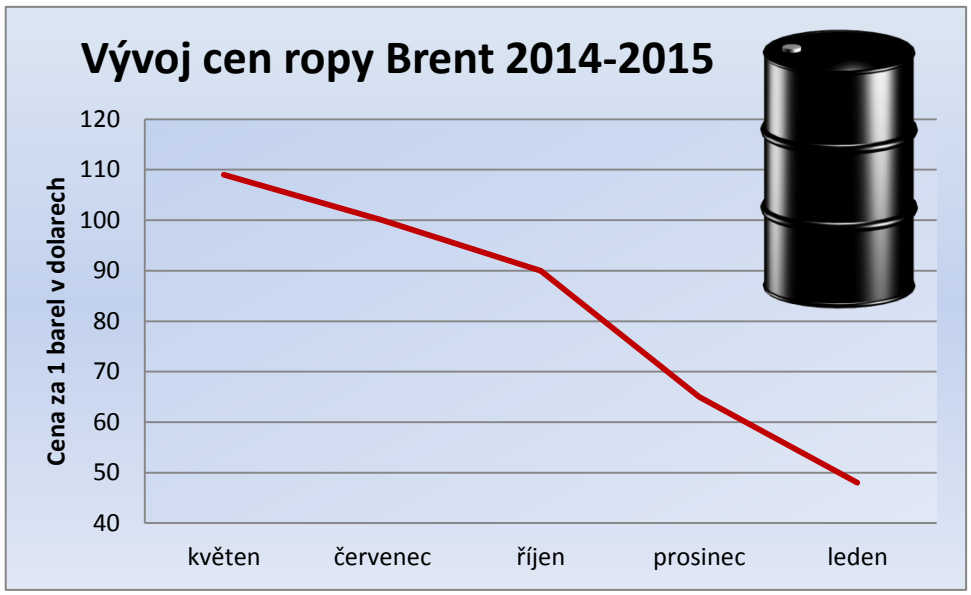
Samotná znalost možností těžby ropy a zemního plynu z břidlic není nikterak nová (v USA se prokazatelně těžil břidlicový plyn již v roce 1825), **ve srovnání s konvenčními způsoby získávání paliv zůstávala ale břidlicová těžba dlouhá léta zoufale neefektivní**. Náklady na získání jednoho barelu ropy přeměnou kerogenu byly dlouho několikanásobně vyšší, než u klasické těžby ve snadno dostupných obrovských nalezištích „hotové“ suroviny např. v Perském zálivu. Obavy vzbuzovaly také dopady nekonvenční těžby na životní prostředí, obrovská spotřeba vody a dalších energií během těžby atd.

O břidlicové ropě a plynu se tudíž hovořilo spíše jako o možných zdrojích v daleké budoucnosti, kdy začnou docházet zásoby konvenčních paliv a ropná nouze svět přinutí přistoupit k dražším a hůře dostupným nekonvenčním zdrojům (odhady toho, jak daleká tato budoucnost má být, se přitom vždy značně rozcházely). Nekonvenční zdroje mají totiž jednu zásadní výhodu – je jich hodně a teoreticky mohou odložit apokalyptický scénář „lidstva bez ropy“ nejméně o celá desetiletí. Odhaduje se, že **z břidlic je možné získat přinejmenším stejné množství ropy jako z konvenčních nalezišť**, v případě břidlicového plynu jsou odhady dokonce ještě optimističtější.

Ve skutečnosti o břidlicové revoluci hovoříme již nyní, tedy v době, kdy je konvenčních zásob uhlovodíkových paliv stále ještě relativní dostatek. **Velká břidlicová naleziště se nacházejí v řadě světových zemí** (Čína, Kanada, Austrálie, Rusko, Argentina, ale také např. Velká Británie či Polsko), nezpochybnitelným **lídrem ve využívání nekonvenčních zdrojů jsou ovšem Spojené státy**, které v posledních několika letech způsobily na poli energetiky doslova převrat. Díky kombinaci několika faktorů (velké investice do nových technologií, které výrazně zlevnily a zefektivnily kdysi nákladnou těžbu; cílená snaha americké administrativy o energetickou nezávislost; poměrně vysoké ceny na počátku dekády, které umožnily prvotní investice do rozvoje nových ložisek) se Američanům podařilo výrazně navýšit vlastní těžbu základních energetických surovin (ropy i zemního plynu) a změnit dlouho zažité vzorce mezinárodních vztahů nejen na poli energetiky.

Proč cena ropy strmě padá

Počátky americké břidlicové revoluce lze datovat ještě před rok 2010, teprve v roce 2014 se ale začaly naplno ukazovat její důsledky, které se projevily zejména **dramatickým pádem cen ropy na světových trzích**. **Od června 2014 do ledna 2015 klesly ceny severoamerické ropy WTI o celých 60%**. Vývoj cen barelu severomořské ropy Brent znázorňuje následující graf.



Jak je vidět, barel ropy Brent se postupně propadl z více než 100$ až na hodnoty pod 50$ za barel, tedy na šestiletá minima z dob hospodářské krize. Podle některých analytiků by se trend měl začít otáčet až ve 3. čtvrtletí roku 2015, do té doby by krátkodobě mohly ceny spadnout až na 20 dolarů za barel (je ovšem možné, že k tomu dojde i mnohem dříve). Obecně se očekává, že se nejpozději v roce 2016 vrátí ceny opět na „udržitelnou“ úroveň, která bývá odhadována kolem 75 dolarů za barel.

Co je příčinou takto dramatického pádu? A jaké jsou jeho důsledky? Současná situace je do značné míry výsledkem psychologické války „tradičních“ těžařů ze zemí kartelu OPEC (v čele se Saúdskou Arábií), s „novými“ břidlicovými těžaři ze Spojených států. Američanům se díky průlomové technologii horizontálních vrtů podařilo snížit náklady a zvýšit efektivitu břidlicové těžby natolik, že **se během pouhých pěti let americká produkce zdvojnásobila**. Je nutné připomenout, že **USA zároveň zůstávají největším spotřebitelem ropy na světě** a až donedávna musely většinu své spotřeby krýt dovozem (mj. ze zemí Perského zálivu, ale také z latinskoamerických států). Obrovský nárůst vlastní produkce způsobil, že Spojené státy už nepotřebovaly dovážet takové množství ropy jako dříve, což způsobilo její přebytek na světových trzích. Výsledkem byl pochopitelně pokles světových cen.

Logickým protitahem velkých arabských producentů by bylo omezení jejich produkce, který by tlak na snižování ceny vyrovnal. K tomu ale nedošlo a především Saúdská Arábie se rozhodla pro zcela jinou taktiku. Zde je nutné si uvědomit, že to byl právě kartel OPEC, který měl po dlouhá desetiletí prakticky monopol na tvorbu ceny na světových trzích – OPEC (Organizace zemí vyvážejících ropu) je sdružením 12 států, které dohromady drží přes tři čtvrtiny světových (konvenčních) zásob. Jejich **neformálním lídrem je Saúdská Arábie, která vlastní zdaleka největší zásoby konvenční ropy na planetě** (a 4. největší zásoby konvenčního zemního plynu). Vzhledem ke své absolutní dominanci mohl OPEC pouhou drobnou úpravou objemu těžby manipulovat s cenami ropy podle svých potřeb (svou sílu kartel demonstroval např. po jomkipurské válce v roce 1973, kdy vyvolal globální ropný šok).

Nečekaným vstupem dalšího silného hráče ztratil kartel OPEC nemalou část své moci nad trhem. Spojené státy navíc na rozdíl od většiny zemí OPEC nejsou „ropným emirátem“ a jejich ekonomika není z drtivé většiny závislá na příjmech z ropného exportu (**v případě Saúdské Arábie tvoří příjmy z ropy 75% příjmů státního rozpočtu**). Pro USA znamená rozšiřování vlastní těžby snižování vlastní energetické závislosti, ale není dominantní silou v národním hospodářství. Naopak pro země OPEC jsou ceny ropy doslova existenčním zájmem.

V konfrontaci s klesajícími cenami ropy po americkém navýšení produkce se Saúdské království rozhodlo svou těžbu nesnížit, což do značné míry předurčilo i reakci dalších zemí OPEC (bez spolupráce s hlavními arabskými producenty jsou možnosti např. Venezuely či Nigérie ovlivňovat cenu velmi omezené). Saúdská Arábie zvolila strategii americké producenty „vyhladovět“, což se z jejího pohledu může jevit jako perspektivnější, než omezení těžby. Za tímto rozhodnutím mohlo stát i odmítnutí na omezení těžby ze strany Ruska (ruská sibiřská ložiska jsou navíc z technologických důvodů velmi neflexibilní a krátkodobé omezení těžby je v jejich případě problematické). Omezením těžby by se sice podařilo zastavit pád cen ropy, ale prakticky by tím OPEC akceptoval vlastní ústup z dosavadního zcela dominantního postavení na trhu a znamenalo by to smíření s novou, pro arabské státy nepříliš příznivou realitou. Namísto toho **se OPEC rozhodl nechat ceny spadnout tak nízko, že se břidlicová těžba přestane americkým producentům vyplácet a jejich podíl na trhu opět klesne** (i přes technologické pokroky je konvenční těžba stále levnější a její regulace jednodušší). Při nízkých cenách nebudou američtí (ani jiní břidlicoví) těžaři schopní investovat do průzkumů nových nalezišť a rozšiřování těch stávajících, což při dlouhých časech nutných pro spuštění břidlicové těžby vyřadí americkou konkurenci na celé roky dopředu.

V takové situaci rozhoduje jediná otázka – kdo vydrží déle? Cena na úrovni pod 60 dolarů za barel žene do ztráty všechny hráče, na americké těžaře ale dopadá víc, díky jejich vyšším provozním nákladům. Na druhou stranu, **pro země OPEC znamená nízká cena obrovské výpadky příjmů jejich národních rozpočtů**, které se propadají do velkého schodku. USA jako celek na ceně ropy existenčně závislé nejsou, země OPEC ano.

Saúdská taktika zatím do značné míry vychází – **počet aktivních amerických břidlicových vrtných souprav klesl na přelomu roku o 7%**. Američtí těžaři zatím ale produkci výrazně nesnižují a doufají, že vydrží déle než OPEC. Ne všechny jeho členské státy mají totiž dostatečné rozpočtové rezervy, aby si takovou cenovou válku mohly dovolit, takže v kartelu to začíná povážlivě skřípat. **Země jako Nigérie či Venezuela se již nyní ocitají ve velkých potížích** a je možné, že zesílí svůj tlak na lídra kartelu Saúdskou Arábii, aby svou strategii přehodnotila. Jak dlouho bude tato válka nervů trvat, je těžké odhadnout. Je ovšem těžko představitelné, že by si některá ze stran mohla dovolit odolávat více než 2 roky. I tak je ale zřejmě faktem, že s americkou břidlicovou revolucí bude nutné počítat i v budoucnosti a geopolitická mapa se díky tomu bude překreslovat.

Globální důsledky nízkých cen ropy

Časopis Times v prosinci 2014 napsal, že pokud cena ropy klesne dlouhodobě pod 50 dolarů za barel, nastolí to nutně na zeměkouli „nový řád“. I z tohoto prohlášení vyplývá, **jak výrazně cena této základní komodity promlouvá do geopolitického uspořádání světa a jak cenová válka mezi Saúdskou Arábií a USA zásadně ovlivňuje zdánlivě nesouvisející bezpečnostní otázky (např. ukrajinskou krizi)**.

Nízké ceny ropy logicky ohrožují především země, jejichž ekonomika je na vývozu této komodity do značné míry závislá, a které si v minulých „tučných“ letech nevytvořily dostatečné rezervy

na horší časy. Hlavních hráčů kartelu OPEC – arabských států v oblasti Perského zálivu - se tak současné změny dotknout paradoxně méně, než by se dalo očekávat, a to přesto, že země jako Saúdská Arábie, Kuvajt či Spojené arabské emiráty jsou na ropě téměř absolutně závislé. Saúdské království se sice letos bude muset kvůli nízkým cenám ropy potýkat se schodkem přes 40 miliard dolarů (skoro bilion korun – tedy prakticky objem celého státního rozpočtu ČR), ale jejich rozpočtové rezervy jsou ve výši 750 miliard dolarů. Země Zálivu si tak mohou dovolit držet si svůj luxusní životní styl po několik let i při nízkých cenách.

Jiným příkladem země, jejíž politická reprezentace myslí i za hranice vlastního volebního období, je Norsko, teoreticky nejpostiženější z evropských států. Růst norského HDP bude v roce 2015 díky nízkým cenám ropy dle odhadů o 1,6% nižší (zatím je norské HDP o 91% vyšší, než je průměr EU). Práci v ropném průmyslu už ztratilo skoro 10 tisíc Norů (celkem jich v tomto sektoru pracuje asi 100 tisíc). **Norové si ale po celých 18 let ukládali své rozpočtové přebytky do zvláštního fondu**, určeného právě pro tyto těžké časy. Podařilo se jim v něm shromáždit astronomických 870 miliard dolarů, což znamená, že i kdyby ceny ropy klesly úplně na nulu, mohli by Norové platit státní výdaje v současném rozsahu ještě dalších pět let.

Ne všechny země ale plánovaly svou budoucnost tak důsledně, případně si mohly dovolit dlouhodobě shromažďovat takové rozpočtové přebytky. **V obrovských potížích se díky současné situace ocitá Nigérie**, která si sice do roku 2008 také vytvořila rezervní fond v hodnotě 20 miliard dolarů, ten se ale za jediný rok smrskl na pouhé 4 miliardy. To znamená, že už v roce 2015 bude mít Nigérie nemalé rozpočtové problémy. To vše za situace, kdy federální vláda čelí velké **bezpečnostní hrozbě ze strany islamistických extremistů z hnutí Boko Haram** (a nad některými částmi země již de facto ztratila kontrolu) a sociální situace v zemi se zhoršuje. Cenová válka tak dost možná ohrožuje samotnou existenci křehké nigerijské federace.

Snad **ještě hůře je na tom Venezuela**, která doplácí na až neuvěřitelně ekonomicky diletantské socialistické experimentování bývalého prezidenta Huga Cháveze a jeho současného nástupce Nicoláse Madury. Země se potýkala s hospodářskými problémy už v předchozích letech, kdy ceny ropy stoupaly vysoko nad 100 dolarů za barel. Vše je o to nepochopitelnější, že Venezuela má zásoby ropy srovnatelné s některými zeměmi Zálivu, životní úroveň obyvatel Dubaje a Caracasu lze ale srovnávat jen těžko. Rozsáhlá korupce a podivné populistické ekonomické a zahraničně-politické excesy způsobily, že si země nevytvořila doslova žádné rozpočtové rezervy a již dnes **se potácí na hranici úplného sociálního kolapsu**. V zemi je nedostatek některých zcela základních komodit (mléko, mouka, toaletní papír, léky atd.) a venezuelská vláda přitom nemá dostatek zahraničních deviz na to, aby tyto nedostatky pokryla dovozem. Inflace dosahuje jedné z nejvyšších úrovní na světě, roste kriminalita a časté jsou výpadky elektrického proudu. Vláda přitom předstírá, že problém v podstatě neexistuje a v monopolizovaných médiích opakovaně chválí vlastní úspěchy. Obrovský odliv mozků do sousední Brazílie a do Spojených států ale půjde zastavit jen velmi těžko a země s velkým přírodním bohatstvím tak stojí na pokraji úplného rozvratu.

Nikterak závratné rozpočtové rezervy nemá ani Irán a existují proto spekulace, že Saúdská Arábie zvolila strategii nízkých cen mimo jiné proto, aby zkomplikovala život svému největšímu regionálnímu rivalovi a případně ohrozila i jeho problematický jaderný program. Zde je zájem Saúdů paradoxně shodný se zájmem USA, proti kterým je jinak saúdské rozhodnutí o zachování současné úrovně těžby namířeno především. A zájmy obou zemí konvergují i jinde. **Ve velmi kritické situaci se ocitá i Rusko**, které v roce 2014 vstoupilo do nepříliš promyšleného zahraničně-politického experimentu na Ukrajině. Před invazí na Ukrajinu mělo Rusko rozpočtové rezervy ve výši zhruba 500 miliard dolarů. Pak ale přišla okupace Krymu a válka na východní Ukrajině, následovaly evropské a americké (ale také kanadské, australské a japonské) sankce, ruské protisankce (které dopadly přinejmenším ve stejné míře na ruské spotřebitele jako na evropské producenty) a **jeho rozpočtová rezerva klesla během jediného roku na 388 miliard**.

Ruská ekonomika je totiž na exportech nerostných surovin mimořádně závislá a výkyvy cen na ní dopadají velmi tvrdě. Někteří analytici a politici označují Rusko dokonce za „plynový emirát“ či „Bangladéš s jadernými zbraněmi“, čímž narážejí na nepříliš moderní uspořádání jeho ekonomiky, které svým důrazem na export primárních surovin odpovídá spíše zemím Třetího světa. Saúdská Arábie tak (zřejmě nechtěně) zasadila smrtící úder nikoliv Washingtonu, ale Moskvě. Někteří příznivci konspiračních teorií, jako je např. spolumajitel Lukoilu Leonid Fedun, se domnívají, že se jedná o saúdsko-americký komplot, což je ale vzhledem k dalším okolnostem velmi nepravděpodobné.

Ruský rozpočet dlouhodobě pracuje s cenami nad 100 dolary za barel, současná úroveň cen ho (v kombinaci s náklady ukrajinské krize) vysává doslova raketovým tempem. Rusko se v roce 2015 propadne do ještě mnohem hlubší recese. Důvěra v rubl silně oslabila, takže centrální banka musela investovat miliardy dolarů na jeho záchranu, v problémech se ocitají největší ruské banky. Pokud země zůstane v mezinárodní izolaci ještě po další dva nebo tři roky, bude situace neudržitelná a Rusko bude nevyhnutelně směřovat k „venezuelskému“ scénáři. Je poněkud paradoxní, že i za této situace ohlašuje prezident Putin rozsáhlé zbrojní programy, které Rusko jednoduše nebude mít z čeho financovat. Ceny ropy tak mají přímé důsledky i na **chování této země v otázce ukrajinské krize**.

Velmi komplikované je vypočítávat důsledky poklesu cen ropy pro Spojené státy. Americká ekonomika není, na rozdíl od té ruské, závislá na jediném zdroji příjmů, a proto **je efekt současné situace pro Američany pozitivní i negativní zároveň**. Nejhůře jsou na tom samozřejmě američtí těžaři a firmy navázané na těžařský průmysl. Jejich akcie prudce padají, například vůbec největší provozovatel ropných plošin a vrtných souprav, **společnost Seadrill, ztratila v roce 2014 skoro tři čtvrtiny své hodnoty**. V Americe také v minulosti hojně investovaly země Perského zálivu, které dnes z logických důvodů své investice omezují. Odchod arabských petrodolarů může americkou ekonomiku zabolet a přinést ztrátu tisíců pracovních míst. Na druhou stranu nejsou USA jen rostoucí producent, ale především největší spotřebitel ropy. A z hlediska spotřebitele je propad cen této komodity jednoznačně dobrou zprávou a pro americkou ekonomiku bude zároveň představovat pozitivní stimul, který by mohl více než vyrovnat i výše zmíněné ztráty amerických těžařů. Tento efekt se projevuje již dnes např. v oblasti chemického průmyslu, který na nízké ceně ropy (tedy důležité vstupní komodity) vydělává. Na něj a na pokles cen je navázána řada dalších odvětví (doprava, zemědělství atd.), což naopak pracovní místa a kapitál generuje. **USA jako celek tak na nízkých cenách ropy spíše vydělávají, než prodělávají**.

Levná ropa může mít ale celou **řadu dalších bezpečnostních i geopolitických důsledků**. Negativně působí například na **aktivity radikálů z islámského státu**, neboť nemalá část z jejich příjmů pochází právě z pašování ropy. Irácká vláda je navíc díky poklesu svých příjmů více tlačena k dohodě s Kurdy. Levná ropa může znovu urychlit zpomalující růst Číny, ale také některých zemí v jihovýchodní a jižní Asii, včetně Indie. Příčiny i důsledky současné situace jsou zkrátka doslova globální.

Možné dopady na Českou republiku

Česká republika patří mezi státy, na které má mít pád cen ropy vesměs pozitivní dopad. ČR je v podstatě čistý dovozce této komodity – **v roce 2014 jsme importovali ropu a ropné produkty v hodnotě kolem 180 miliard Kč**. Při ceně pod 60 dolarů za barel ropy Brent by se tato částka snížila skoro o třetinu. Jenže skutečný efekt pro ČR není tak jednoduché vyčíslit. Nižší ceny ropy snižují náklady v řadě odvětví, což funguje jako pozitivní stimul pro růst ekonomiky. Faktorů, které vstupují do hry je ale více - např. **vývoj kurzu české koruny**, který může celkový efekt částečně tlumit nebo naopak posílit.

Situace je pochopitelně výhodná pro dopravce a motoristy, třebaže pokles cen pohonných hmot na čerpacích stanicích nemusí být (a také není) zdaleka tak dramatický, jako pád ceny vstupní komodity na burzách. Ještě mnohem více se tak pozitivní efekt projeví v případě průmyslu, který nakupuje tuto surovinu ve větším množství – v ČR zejména **chemické závody, producenti umělého textilu a plastů**. **Náklady ovšem klesají také v zemědělství a v důlním sektoru**. Podle odhadů banky Citigroup sníží 20% pokles cen ropy výrobní náklady na tunu černého uhlí zhruba o 10%. **Obecně situace nahrává nejen firmám a podnikům, které zpracovávají ropu, ale také které mají vysoký podíl spotřeby energií na celkových nákladech (např. sklárny, hutě, těžké strojírenství atd.)**. Díky snížení hodnoty celkového dovozu se také zlepšuje obchodní bilance ČR

Dopady na ČR ovšem nemusí být jen čistě pozitivní. Velký propad cen základních energetických surovin může srazit nízkou inflaci do záporných čísel, tedy **způsobit deflaci**. A deflace není nic, z čeho mají ekonomové radost. Při poklesu cen lidé odkládají nákupy na pozdější dobu (čekají na ještě nižší ceny), roste reálná hodnota dluhů, takže firmy si nechtějí brát úvěry a omezují investice. Deflace proto může ekonomiku jako celek naopak zpomalit.

Celkově se nicméně odhaduje, že **nízké ceny meziročně posílí růst českého HDP zhruba o 0,3 - 0,7 %**. Propad cen ropy je pro ČR vcelku pozitivní, musíme si ale uvědomit, že tak jako ceny této komodity v nedávné době spadly, mohou (jak se to v minulosti stalo několikrát) v budoucnu zase raketově narůst. Je tedy celkově dobré **usilovat o maximální diverzifikace a vyvarovat se absolutní závislosti na jedné energetické surovině**.

Cvičení DRILL 2014

Dne 16. září 2014 proběhlo v blízkosti hraničního přechodu Hora Sv. Šebestiána, okres Chomutov, mezinárodní taktické **cvičení „DRILL 2014“**, které **simulovalo situaci významného ohrožení bezpečnosti a spolehlivosti elektrické přenosové soustavy v důsledku poruchy mezinárodního propojovacího vedení se Spolkovou republikou Německo** a možných souvisejících mimořádných událostí. Cílem cvičení bylo procvičit koordinovaný zásah složek integrovaného záchranného systému s využitím poplachového plánu pro daný region hranice se SRN při likvidaci následků živelní pohromy a souvisejících mimořádných událostí a připravenost provozovatelů přenosových soustav obou zemí při obnově strategického vedení. Vlivem extrémně nepříznivých klimatických podmínek došlo k destrukci dvou kotevních hraničních stožárů dvojitého propojovacího vedení V445/V446 z Čech do Saska.

Bylo rozhodnuto o okamžitém zahájení koordinované výstavby náhradní přenosové trasy s cílem uvést poškozené mezinárodní vedení co nejdříve do provozu. S ohledem na nepřístupnost terénu a urychlení výstavby **bylo nutné pro přepravu vybraných komponent využít vrtulník AČR**. Situaci na místě zásahu značně komplikoval **požár lesního porostu**, který vznikl při bouřce a následném elektrickém výboji. JPO obou zemí se společně podílely na likvidaci požáru v blízkosti státní hranice. PČR řídila dopravu a realizovala opatření na státní hranici. Za Krajské ředitelství policie Ústeckého kraje se cvičení zúčastnili policisté služby pořádkové a dopravní policie, policisté integrovaného operačního střediska, policisté skupiny krizového řízení, pracovníci OIKT, překladatelka a tisková mluvčí. Do cvičení bylo dále zapojeno 13 českých jednotek profesionálních i dobrovolných hasičů, 3 jednotky ze SRN, Zdravotnická záchranná služba Ústeckého kraje, Letecká služba Policie ČR, Policie SRN, Armáda ČR, THW SRN, společnost ČEPS a společnost 50 Hertz. Celkem **dohromady cca 31 zásahových a technických vozidel a 143 cvičících osob**.

Vybrané události ve sledovaném období

Červenec

Odpojení Temelína ze sítě kvůli poruše čerpadla

Druhý blok jaderné elektrárny Temelín byl v červenci odpojen od rozvodné energetické sítě kvůli poruše čerpadla. První blok byl ve stejné době již měsíc odstaven kvůli výměně paliva. Společnosti ČEZ se podařilo dodávky pokrýt z jiných zdrojů, takže se událost nedotkla odběratelů elektřiny. Temelín za běžného stavu dodává asi 20% české spotřeby.

Důvodem odstávky druhého výrobního bloku byla porucha jednoho ze dvou čerpadel prvního systému technické vody důležité v nejaderné části elektrárny k chlazení technologických zařízení. Elektrárna má celkem tři na sobě nezávislé okruhy technické vody – tzv. „technická voda důležitá“ je pro chod elektrárny klíčová. U odstaveného prvního bloku zároveň probíhala modernizace, která zvýšila výkon z 1056 MWe na 1078 MWe, aniž by zároveň došlo k nárůstu množství spotřebovaného paliva.

Vandal navrtal nový teplovod v Čáslavicích

V Čáslavicích na Třebíčsku navrtal neznámý vandal desítky děr do nového teplovodu za devět milionů korun. Stavba měla rozvádět teplo ze zemědělské bioplynové stanice k domům v obci. Původně měla napájet 15 domů, radnice ale do budoucna uvažovala o jejím rozšíření. Stavba se prováděla zároveň se stavbou nové kanalizace a obměny elektrické sítě, na poškození se ale přišlo až při tlakové zkoušce, kdy byly výkopy již částečně zasypány. Ty je nyní nutné znovu odkrýt a poškozené potrubí vyměnit.

Práce na teplovodu se tak protáhnou až do začátku topné sezóny a navíc budou dál komplikovat život v obci. Za poškozením plynovodu mohla stát závist, neboť obec nemohla vyhovět všem zájemcům o připojení. Roli údajně hráli technické podmínky. Většina domů připojených na nový teplovod tak patří členům družstva. Pachateli hrozí až šest let vězení. Družstvo na jeho dopadení dokonce vypsalo odměnu.

Srpen

ČEZ dokončil paroplynovou elektrárnu v Turecku

Skupina ČEZ spolu s partnerem, tureckou společností Akkök, převzali od dodavatele nově vystavěnou paroplynovou elektrárnu Egemer na jihovýchodě země a zahájili tak přímý provoz. Mimořádně efektivní zdroj s účinností přesahující 57 % a životností minimálně 30 let by měl ročně vyrobit až 7000 GWh elektrické energie.

Výstavba paroplynového zdroje o celkovém instalovaném výkonu 872 MW byla zahájena na podzim 2011 a dokončena i navzdory náročnému terénu přesně podle plánu. Již během zkušebního provozu totiž začala elektrárna dostávat za elektřinu dodanou do sítě zaplaceno díky speciálnímu povolení od Ministerstva energetiky. Jen to přineslo dodatečné úspory v řádu stovek milionů korun. Ušetřit se ale podařilo i snížením souvisejících výdajů na financování projektu a také menší spotřebou plynu během najíždění.

Při výstavbě bylo třeba se vypořádat s řadou překážek, zejména s velmi náročným terénem – elektrárna totiž stojí na pláži, jen necelý kilometr od Středozemního moře. Bylo tedy nutné stabilizovat povrch písečné pláže zapuštěním 1100 betonových pilot sahajících až do hloubky 35 metrů a dalších 10 000 sypaných štěrkových pilot hlubokých 20 metrů, která snižují rizika poruch podloží při zemětřesení. Díky této unikátní poloze však může být elektrárna chlazena přímo mořskou vodou. Přivaděč vody je veden 1,5 kilometru po mořském dně. Jednotlivé komponenty elektrárny byly dodávány z celého světa – generátory z USA, plynové turbíny z Francie a parní z Čech, kotel z Jižní Koreje. Kromě samotné elektrárny byly vybudovány také linky pro vyvedení výkonu v celkové délce 34 km a 17kilometrová plynová přípojka.
Skupina ČEZ zahájila své podnikání v Turecku v roce 2008 podpisem o strategické spolupráci se společností Akkök Group. Společný podnik Akenerji provozuje dvě paroplynové, jednu větrnou a osm vodních elektráren o celkovém instalovaném výkonu přes 1,5 GW. Výrobní firma dosahuje již dva roky po sobě rekordních provozních zisků (v roce 2013 1,8 mld. Kč). Daří se zde i v oblasti distribuce, ČEZ se svým partnerem Akkök dodává elektřinu 1,4 milionu zákazníků v jedné z nejprůmyslovějších oblastí na severozápadě Turecka.

Září

Policie cvičila ochranu Temelína

Maskovaní policisté, střelba nebo dýmovnice. Tak vypadala jedna z ukázek pracovního setkání, které dnes proběhlo v Jaderné elektrárně Temelín. Představitelé Státního úřadu pro jadernou bezpečnost, Integrovaného záchranného systému, krajské správy, samosprávy a Jaderné elektrárny Temelín probírali poučení z událostí JE Fukušima. Nechyběl ani zástupce Evropské komise. Dynamickou tečku za setkáním udělala Policie ČR. Poprvé za přítomnosti médií předvedla zadržení osob, které neoprávněně pronikly do areálu největší české elektrárny.
Krátce po druhé hodině dvě osoby překonávají plot areálu elektrárny. Následuje kolotoč přesně stanovených kroků. Část policistů v kuklách zajišťuje strategické budovy. Situaci sleduje ukrytý policejní odstřelovač. Ten také dává informaci zasahujícímu týmu. Akce trvá čtyři minuty. Narušitelé jsou zadrženi. V poutech jsou převáženi k dalšímu výslechu do Českých Budějovic. Fyzická ochrana elektrárny Temelín byla opakovaně prověřována mezinárodními odborníky. Poslední prověrka proběhla v roce 2008 a inspektoři tehdy zařadili Temelín mezi špičku jaderných elektráren z pohledu fyzické ochrany.

V teplárně Vítkovice unikla v rámci cvičení kyselina chlorovodíková

V areálu Teplárny Vítkovice proběhlo havarijní cvičení. V jeho rámci došlo vlivem netěsnosti spojovacího potrubí ze zásobních nádrží kyseliny chlorovodíkové k jejímu úniku. V souvislosti s touto událostí byl zraněn jeden ze zaměstnanců provozu. O vzniku mimořádné události bylo neprodleně informováno operační středisko Hasičského záchranného sboru města Ostravy, vzápětí následoval výjezd hasičů k místu ekologické havárie.
Únik kyseliny simuloval kouřový doutnák, roli zraněného zaměstnance teplárny zastala figurína. Zaměstnanci Teplárny Vítkovice i členové Hasičského záchranného sboru během fingované havárie obstáli a předvedli bezchybnou práci. Cvičení potvrdilo připravenost zapojených složek teplárny řešit podobné události tak, aby byly minimalizovány dopady nehod na životy a okolní prostředí. Teplárna

Vítkovice vyrábí takzvaným teplárenským způsobem teplo i elektrickou energii z černého uhlí. Její tři kotle disponují celkovým výkonem 342 MWt. Čtyři instalované turbíny disponují výkonem 79 MWe. Roční produkce elektřiny činí cca 100 tisíc MWh a roční produkce tepla činí cca 1 mil.GJ.

Cvičení SAFEGUARD v Kletné

Účastníci museli čelit útoku protivníka a následně uchránit transformační uzel v Kletné na Novojičínsku, který je důležitý pro stabilitu dodávek elektřiny do okolního regionu. Jeho provoz nebyl cvičením nijak dotčen. Vše se odehrávalo v naprosto reálných podmínkách, vycházejících ze skutečných scénářů možného ohrožení. V jeho rámci bylo představeno několik dynamických zásahů, součástí byla demonstrace způsobu ochrany transformovny příslušníky AČR při napadení ozbrojenou skupinou útočníků za použití vrtulníku. PČR předvedla zásah v případě ohrožení chodu transformovny aktivisty, kteří blokují vstup do objektu. Došlo i na řešení situace použití nebezpečných látek, které ohrozily chod transformovny, a snížily tak spolehlivost dodávek energie v kraji. Příslušníci HZS provedli prvotní průzkum terénu, monitoring ovzduší, odběr vzorků a následnou chemickou analýzu v mobilní laboratoři.
Cvičení SAFEGUARD 2014 ověřilo praktickou připravenost jednotky pěší roty aktivní zálohy krajského vojenského velitelství Ostrava a jejich spolupráci s pracovníky společnosti ČEPS. Vojáci převzali obranu a střežení transformovny Kletné po dobu několika dní. Během nich plnili úkoly strategické obrany v prostorách transformovny i v jejím okolí a zároveň zajišťovali fungování vlastního vojenského logistické zázemí. Při cvičení využívali také leteckou podporu vojenského vrtulníku. Do scénáře cvičení byl zahrnut i zásah speciální pořádkové jednotky Policie ČR Moravskoslezského kraje proti skupině aktivistů, kteří zablokovali přístup do transformovny. V průběhu krizového vyjednávání došlo ze strany aktivistů k napadení zasahujících policistů. Současně s tím aktivisté na místě ohrožovali zasahující jednotky neznámou nebezpečnou látkou. Proto byla do akce nasazena speciální protichemická jednotka Hasičského záchranného sboru Moravskoslezského kraje, která odebrala vzorek, zanalyzovala jej v mobilní laboratoři a nebezpečnou látku zlikvidovala.
SAFEGUARD je název série bezpečnostních cvičení, která prověřují spolupráci Armády ČR, složek integrovaného záchranného systému a společností ČEPS a ČEZ. Taková cvičení proběhla již v minulosti například v transformovnách Nošovice a Albrechtice.

Říjen

ČEZ se dohodl s Albánií o narovnání

Na půdě Sekretariátu energetického společenství ve Vídni si strany vzájemně potvrdily splnění všech odkládacích podmínek, čímž vstoupila v účinnost dohoda o narovnání uzavřená mezi společnostmi Skupiny ČEZ a Albánií v červnu tohoto roku. Podle ní ČEZ získá celkem 100 milionu EUR, tedy částku obdobnou počáteční investici do nákupu albánské distribuční společnosti.
Podle uzavřené dohody obdrží Skupina ČEZ za úhradu pohledávek a převod podílu v distribuční společnosti kompenzaci 85 milionů EUR, dalších 15 milionů EUR již společnost obdržela. Částka bude vyplácena do roku 2018 v ročních splátkách, které jsou kryty garancí renomované evropské banky. Dnem nabytí účinnosti dohody byl převeden i 76% podíl společnosti ČEZ v distribuční společnosti zpět na albánský stát. V návaznosti na účinnost dohody bude ukončena i arbitráž vedená proti Albánii, kterou zahájil ČEZ v květnu minulého roku kvůli neochráněné investici do distribuční společnosti.

Prověření havarijní připravenosti v elektrárně Prunéřov

Únik sádrovcové suspenze a její průnik do dešťové kanalizace v elektrárně Prunéřov I zalarmoval požární hlídku příslušné směny v provoze, podnikové hasiče i celý havarijní štáb. Událost zaznamenal jeden z pracovníků elektrárny při běžné kontrole potrubí, který ihned informoval směnového inženýra. Ten vzápětí spustil nezbytný proces, jímž byly všechny dotčené osoby a instituce informovány o vzniku mimořádné události s dopadem na životní prostředí. Jednalo se přitom o další havarijní cvičení v uhelných elektrárnách Skupiny ČEZ na severu Čech.

Simulovaný únik sádrovcové suspenze byl zaznamenán v 8:58 hodin, bezprostředně poté vyslal směnový inženýr na místo požární hlídku, jakmile byl obeznámen se skutečným stavem věci, okamžitě informoval elektrárenské hasiče. Na ohlašovně požárů přitom přijali informaci o mimořádné situaci v 9:05 hodin, přičemž o tři minuty později již byli prunéřovští hasiči na místě a likvidovali následky havárie. Jejich tušimickým kolegům, které „požádali“ o pomoc, pak stačilo pouhých dvanáct minut na to, aby se rovněž mohli zapojit do akce. V jejich případě se jednalo o ověření času dojezdu ze stanice v Elektrárně Tušimice, přičemž by případně zasahovali přímo v absorbéru odsíření. V 9:26 hodin již byla učiněna veškerá opatření a místo pomyslné ekologické havárie se jen monitorovalo.

Simulované zneškodňování výbušniny na vodní elektrárně Kamýk

Nález neznámého předmětu v útrobách vodní elektrárny Kamýk odstartoval včera celou sérii událostí, jež prověřily souhru Policie ČR, obsluhy elektrárny a Havarijního štábu provozu. To byl ostatně hlavní cíl havarijního cvičení, které celou situaci navodilo. Vodní elektrárna Kamýk, která ročně vyrobí v průměru 80 milionů kWh a pokryje tak spotřebu 23 tisíc středočeských domácností, prošla v uplynulém roce největší modernizací za celou dobu jejího 53letého provozu. Po vyhlášení mimořádné události v areálu elektrárny dorazili přítomní zaměstnanci elektrárny a dozorství přehrady Kamýk dle pokynů člena Havarijního štábu na určená shromaždiště, zatímco souběžně zasedající Havarijní štáb provozu vyrozuměl zástupce Povodí Vltavy, ředitele Organizační jednotky Vodní elektrárny ČEZ, a. s., a specialistu fyzické ochrany vodních elektráren. Na pokyn předsedy Havarijního štábu provozu byl zpracován jmenný seznam přítomných osob, připraveny operativní karty obsahující schémata elektrárny a připraveny náhradní komunikační prostředky pro potřeby složek Policie. O vzniku mimořádné události bylo vyrozuměno středisko Centrály nouzové služby, které ihned vyslalo na Kamýk pracovníka bezpečnostní agentury. Personál elektrárny si tak mohl nanečisto vyzkoušet postupy při odvracení teroristické hrozby. Policejní hlídka z obvodního oddělení Milín prověřila pravdivost oznámení a vzápětí požádala o příjezd posilových hlídek, které zajišťovaly uzávěru kolem Vodního díla Kamýk. K nálezu byl současně povolán pyrotechnik a psovod se psem, který se specializuje na vyhledávání výbušnin. Pyrotechnik zneškodnil první nástražný systém umístěný na turbínovém víku TG4 a balíček tak mohl být převezen mimo objekt elektrárny do areálu blízké pískovny k řízené likvidaci. Současně psovod za pomoci policejního psa odhalil ještě druhou „bombu“ ukrytou v technologickém zázemí rychlozávěrů vtoků – také na TG4. I tento pekelný stroj putoval k řízenému zničení. Celé cvičení trvalo 3 hodiny a 25 minut.

Záhadné drony nad francouzskými jadernými elektrárnami

Francie vyčlenila milion eur na vývoj technologií k odhalení a zachycení malých bezpilotních letadel, která od října 2014 záhadně přelétávají nad tamními jadernými elektrárnami. V říjnu a listopadu 2014 bylo zaznamenáno nejméně dvacet takových přeletů. Francie má v rámci devatenácti elektráren 58 jaderných reaktorů a tamní zákon zakazuje přelétat tyto a další strategické objekty v okruhu pěti kilometrů ve výšce pod 1 000 metrů. Malé civilní bezpilotní stroje, které si je již možné pořídit na běžném trhu a létají nízko nad zemí, nelze odhalit radary. Majitelé je řídí dálkově nebo mohou jejich let naprogramovat.

Rusko bude příštích 15 let dodávat ropu na Slovensko

Slovensko si na dalších patnáct let nasmlouvalo ropu z Ruska. Rámcová dohoda počítá s dodávkami až šesti milionů tun ropy za rok. Smlouvu podepsali ruský ministr energetiky Alexandr Novak a jeho slovenský protějšek Pavol Pavlis.

Podle rusko-slovenské smlouvy bude Rusko mezi 1. lednem 2015 a 31. prosincem 2029 dodávat ropovodem Družba každoročně až šest milionů tun ropy. Podle dohody, kterou ruská vláda schválila 30. října, bude stejné množství proudit také přes Slovensko do dalších evropských zemí.

Zahraniční kontrolní mise v jaderné elektrárně Dukovany

Na deset dnů přijelo 7 expertů a 4 pozorovatelé z 10 zemí do JE Dukovany, aby prověřili její připravenost k dalšímu dlouhodobému provozu. Kromě posouzení souladu mezinárodních doporučení, předají také specialisté mise SALTO (Safety Aspects of Long Term Operation – bezpečnostní aspekty prodlužování provozu za hranici životnosti) znalosti a zkušenosti s touto problematikou pro zlepšení produktivity činnosti v oblasti prodlužování životnosti Dukovan. Součástí mise bude také posouzení vypořádání návrhů a doporučení z poslední tematicky obdobné mise v roce 2011. Závěry z mise byly následně předány vedení elektrárny. Zpráva z této mise bude jedním z podkladů k žádosti o povolení dalšího provozu 1. bloku EDU, které budou předkládány SÚJB v roce 2015.

Loď Arctic Sunrise má po Rusku problémy i ve Španělsku

Loď Arctic Sunrise, kterou ruské úřady loni zabavily mezinárodní ekologické organizaci Greenpeace při protestu aktivistů u ruské těžební plošiny v Barentsově moři, se dostala do nových potíží. Na Kanárských ostrovech ji pro změnu zablokovalo Španělsko poté, co vplula do zakázané námořní zóny, kde začal podmořský průzkum možných ropných zdrojů. Podle španělské vlády plavidlo Greenpeace nerespektovalo zákaz pro plavbu a rybaření ve vyhrazené zóně a dostalo zákaz opustit přístav v Arrecife na Kanárských ostrovech, dokud kapitán lodi, jímž je Američan, nezaplatí kauci 50 000 eur (1,4 milionu Kč). Tři plavidla španělského námořnictva zadržela již v sobotu několik členů Greenpeace operujících ze základní lodi Arctic Sunrise, které se pokoušely přiblížit k průzkumné lodi energetické společnosti Repsol. Při incidentu natočeném Greenpeace na video spadla jedna z aktivistek hnutí do moře.

Od loňského září, kdy byla během zásahu ruského ozbrojeného komanda zadržena třicetičlenná posádka Arctic Sunrise, Rusko loď blokovalo do letošního srpna. Ruské úřady zásah nařídily kvůli údajně nelegálnímu protestu u ruské ropné plošiny Prirazlomnaja. Všichni aktivisté, z toho 26 cizinců, byli do konce loňského listopadu v ruské vazbě. Poté je pustil soud na kauci na svobodu, ale nesměli opustit Rusko. Trestní stíhání všech zadržených - zprvu za pirátství a posléze za výtržnost - ukončila až amnestie. Tu vyhlásili v prosinci 2013 ruští poslanci na návrh prezidenta Vladimira Putina. Aktivisté po vyřízení formalit z Ruska odcestovali.

Cvičení v teplárně Trmice simulovalo únik oleje do čističky

Dle scénáře cvičení došlo krátce po deváté hodině ranní v trmické teplárně k požáru olejového hospodářství v suterénu strojovny a následnému úniku oleje do čističky odpadních vod. K zásahu okamžitě vyjela jednotka hasičů Teplárny Trmice k likvidaci ohniska požáru i zabránění ekologické havárie. Zaměstnanci teplárny spolu s podnikovými hasiči zabránili úniku oleje do řeky Bíliny instalací norných stěn v záchytné jímce čističky odpadních vod. Následně došlo k likvidaci zachycených olejových látek.

Teplárna Trmice patří do Skupiny ČEZ, je zde instalováno 6 kotlů o celkovém tepelném výkonu 469,2 MWt a 6 turbogenerátorů na výrobu elektrické energie o výkonu 89 MWe. Do města Ústí nad Labem dodává teplárna 3700 TJ tepelné energie v páře za rok. Celkem je k ní připojeno více

než 1300 odběrných míst. Teplem zásobuje zhruba 27 tisíc domácností a na tři desítky průmyslových podniků ve svém okolí.
Podobné cvičení se ve stejném měsíci uskutečnilo i v elektrárně Tisová, kde měla ze spojovacího potrubí zásobních nádrží HCl uniknout do prostoru kolejiště kyselina chlorovodíková. Proběhl zásah hasičů ve speciálních ochranných oděvech, který spočíval ve skrápění oblaku kyseliny sírové a současně jejím ředění. Nebezpečná kyselina byla poté přečerpána do záložní nádrže.

Nehoda v ukrajinské jaderné elektrárně Záporoží
Jeden z reaktorů Záporožské jaderné elektrárny na jihovýchodě Ukrajiny vyřadila z provozu nehoda. Jedná se o vůbec největší jadernou elektrárnu v Evropě, která zaměstnává přes 11 tisíc lidí. Generuje asi polovinu jaderné energie na Ukrajině a více než pětinu z celkové elektrické energie vyrobené v zemi. Potíže se podle ukrajinského ministra energetiky netýkaly samotné produkce elektrické energie, ale vnitřních energetických rozvodů, kde nastal zkrat. Jaderná bezpečnost podle tohoto vyjádření nebyla ohrožena. Poškozený blok byl odpojen od elektrické soustavy. Odstávka třetího bloku záporožské elektrárny ještě více zhoršila už tak špatnou energetickou situaci v zemi. Kvůli potížím s distribucí energie ministr Demčyšyn požádal velké průmyslové odběratele, aby dobrovolně snížili svou spotřebu.

Hasiči na Orlíku v rámci cvičného požáru slaňovali hráz přehrady

Simulovaný požár v kabelové šachtě jednoho z hrázových bloků zalarmoval příbramské hasiče, aby dorazili do největší české klasické vodní elektrárny Orlík. Tematické havarijní cvičení prověřilo souhru jednotek Hasičského záchranného sboru s obsluhou elektrárny a se specialisty Povodí Vltavy. Hasiči také využili zásahu pro atraktivní nácvik slaňování 100metrové hráze. Vodní elektrárna Orlík loni dodala do sítě 554,5 milionů kWh elektřiny, a pokryla tak spotřebu více než 150 tisíc domácností v regionu na pomezí středních a jižních Čech.
Havarijní cvičení na Elektrárně Orlík patří do pestrého kalendáře akcí podobného druhu. Od ledna do listopadu 2014 proběhla cvičení na 21 klasických a vodních elektrárnách Skupiny ČEZ. V rámci cvičení zjistila krátce po osmé hodině ráno obsluha požár v prostoru svislého kabelového kanálu v hrázovém bloku číslo 19. Pracovník obsluhy po prověření stavu bleskově informoval Hasičský záchranný sbor, Dispečink Vodních elektráren, pracovníka pohotovosti a vedoucího provozu. Následně tuto informaci obdržel také podnikový technik požární ochrany a ředitel Vodních elektráren. Za necelých 20 minut dorazila na elektrárnu jednotka profesionálů z HZS Příbram. Součástí havarijního cvičení byl výcvik lezecké skupiny HZS Středočeského kraje v boční části 91,5metrové hráze. Hasiči postupně slaňovali k patě hráze, aby nacvičili rychlé dosažení budovy elektrárny.

Prosinec

Na Karlovarsku a Sokolovsku vyhlásili energetici kalamitu, v Praze přestaly jezdit tramvaje
Kvůli pádům stromů i elektrického vedení se počátkem prosince v Krušných horách ocitly stovky domácností bez proudu. Stromy a dráty obalené ledem způsobovaly velké potíže v celém Karlovarském kraji. Situace byla vážná také v jižních Čechách a na jižní Moravě. V Praze kvůli ledovce dokonce úplně zkolabovala tramvajová doprava, když ledovka pokryla trolejové vedení a řada souprav zůstala stát přímo na ulicích. Podobnou situaci nezažila Praha několik desítek let.

V Brně řádil falešný energetik
Dvacetiletý mladík, který se vydával za zástupce energetické firmy, zvonil na obyvatele brněnské čtvrti Žabovřesky a místním lidem tvrdil, že jejich stávající smlouvy jsou neplatné. Několika starším občanům dokonce vyhrožoval, že pokud nepodepíší smlouvy nové, bude jim odpojena elektřina. Pokud jeho nabídku lidé odmítli, choval se velmi hrubě, případně reagoval tím, že je kontrolor a pouze ověřoval, zda někdo neobtěžuje klienty s nevyžádanými nabídkami. Muže dopadli strážníci ve chvíli, kdy se pokoušel uzavřít smlouvu s pětaosmdesátiletým seniorem.

Vláda povolila možnou těžbu uranu na Vysočině
Vláda schválila návrh ministra průmyslu a obchodu Jana Mládka o přípravě těžby uranu u Brzkova na Jihlavsku. V České republice je v současné době v provozu vůbec poslední uranový důl ve střední Evropě – v Rožné na Žďársku. Ročně vyprodukuje zhruba dvě stě tun uranu, ukončení těžby se nicméně předpokládá v horizontu tří let. Důl v Rožné v současné době zaměstnává asi tisíc lidí, z nichž někteří by mohli najít práci v padesát kilometrů vzdáleném Brzkově. V této lokalitě proběhla průzkumná těžba už v 80. letech, teprve nyní ale bylo rozhodnuto o možné využití ložiska. Nový důl by mohl začít fungovat od roku 2022.
Obyvatelé okolních obcí ale proti těžbě protestují a premiérovi předali petici se 1700 podpisy. Těžbu odmítají i ekologické iniciativy, které se navíc obávají jejího rozšíření i do severních Čech (v okolí Liberce a České Lípy), kde jsou ložiska ještě pětinásobně větší než v Brzkově. Obávají se technologie kyselinového loužení, které údajně vede k zamoření podzemních vod. Ministr Mládek ale chemickou těžbu v této lokalitě vylučuje.

Dokončení rekonstrukce malé vodní elektrárny v Brně-Komíně

Modernizace a opravy nejdůležitějších technologií i kompletní rekonstrukce kamenné navigace – to jsou výsledky tříměsíčních prací na malé vodní elektrárně v Brně-Komíně. Ekologický provoz tak bude moci spolehlivě pokračovat v roční výrobě elektřiny pro 200 domácností a současně sloužit jako vyrovnávací zdroj pro elektrárnu na Brněnské přehradě. Malá elektrárna funguje na řece Svratce už od roku 1923. Kromě repasování technologií obou soustrojí došlo na opravu nábřežních stěn objektů náhonu, jalové propusti a odpadního kanálu, které byly poškozeny stářím, působením klimatických podmínek a vodní erozí. V tomto rozsahu byly práce provedeny poprvé za 91 let provozu elektrárny. Ta ročně vyrobí přes 700 tisíc kWh elektřiny.

ČEZ zastavuje provoz ve své uhelné elektrárny v Bulharsku
Česká společnost ČEZ bude v roce 2015 nucena zastavit provoz své uhelné elektrárny v bulharské Varně. Bulharsko nezískalo povolení pro krátkodobý provoz, protože zařízení nesplňuje ekologické limity. Elektrárna ve Varně má šest bloků o výkonu 210 megawattů, energii ale vyrábí jen v omezeném rozsahu, protože funguje jako záložní zdroj energie. Neplní limity pro emise oxidů dusíku a síry. Začátkem listopadu ČEZ informoval o tom, že se s bulharskou státní energetickou společností Bulgarian Energy Holding (BEH) nedohodl na financování modernizace varnské elektrárny.
Brusel připustil výjimku pouze za situace, kdyby nastala plynová krize. ČEZ tak postupně propustí všech 300 zaměstnanců elektrárny a začne hledat případného kupce. Pokračují tak problémy společnosti v Bulharsku – po protestech proti údajně předraženým cenám elektřiny, které přerostly v celonárodní politickou krizi, místní parlament schválil změny, které umožnily snížení ceny. Bulharský antimonopolní úřad následně obvinil ČEZ a rakouskou firmu EVN ze zneužití postavení na trhu a nastavení nesmyslně vysokých cen.

Únik plynu uzavřel liberecké náměstí
Hasičský záchranný sbor byl nucen evakuovat pět domů kvůli úniku plynu na Benešově náměstí v Liberci. Přerušeno bylo také konání místních vánočních trhů. Podle hasičů došlo k poruše na kabelu vysokého napětí, který vedl blízko plynovodu, což se projevilo mírnou tlakovou vlnou. Hasiči zásah ukončili po ujištění plynařů, že nebezpečí nehrozí. Lidé se tak mohli vrátit do svých domovů, byl zprovozněn trh a znovu zapojena elektřina.

Slovensko vypoví smlouvu o pronájmu vodní elektrárny Gabčíkovo
Slovenská vláda se rozhodla vypovědět společnosti Slovenské elektrárny, kterou ovládá italský koncern Enel, smlouvu o dlouhodobém pronájmu největší vodní elektrárny v zemi Gabčíkovo. Oznámil to slovenský premiér Robert Fico. Podnik podle něj porušuje smlouvu o provozování tohoto vodního díla. Slovenské elektrárny premiérovy výtky odmítly.
Slovenské elektrárny získaly vodní dílo Gabčíkovo na řece Dunaj k 30letému pronájmu během privatizace podniku v roce 2006. Podle Fica na něm za osm let vydělaly 340 milionů eur. Podnik má dle smlouvy nárok na 35 procent příjmů, zbytek připadá státu. Instalovaný výkon elektrárny činí 720 megawattů.

Rusko dodá Indii 12 jaderných reaktorů
Na summitu v hlavním městě Indie byla uzavřena dohoda mezi ruskou státní společností Rosatom a indickými zástupci, že v příštích dvaceti letech zajistí Rosatom výstavbu dvanácti jaderných reaktorů. Šest jich bude stát v provincii Tamilnádu, o umístění dalších šesti se teprve bude rozhodovat. Úspěch měla i ropná firma Rosněft, ta má dodat během deseti let deset milionů tun ropy.
Dohoda o jaderných reaktorech má posílit spolupráci v jaderné energetice mezi oběma zeměmi. V indickém Tamilnádu už Rosatom první reaktor s výkonem tisíc megawattů pro jadernou elektrárnu Kudankulam postavil, druhý by měl být zprovozněn v roce 2015. Indičtí představitelé uvádějí, že by v Kudankulamu mělo být dohromady šest reaktorů. Lokalita, kde budou postaveny další reaktory, zatím nebyla vybrána.
Na Rusko těžce dopadá kombinace západních sankcí a nízkých cen ropy, takže hledá nové příležitosti pro oživení vlastní ekonomiky.

***Zdroje pro tuto kapitolu**: MV, MPO, vlada.cz, prumysl.cz, ČT24, lidovky.cz, novinky.cz, kyivpost.com, ppas.cz, ceps.cz, cez.cz, ceskatelevize.cz, akualne.cz, idnes.cz, enviweb.cz, tretiruka.cz, janes.com, ceskenoviny.cz, rozhlas.cz, reko a.s., e15.cz, euraktiv.cz, atominfo.cz, ČTK, energydigital.com, PČR, GŘ HZS ČR, sxc.hu, govcert.cz, spiegel.de, bihdaytonproject.com, eskom.co.za, aawsat.net, rijmenants.blogspot.cz, byznys.ihned.cz, praha.idnes.cz, article.wn.com/view, swissinfo.ch, wbir.com, oakridgetoday.com, wikipedia.org, ekonomika.idnes.cz, thermoil.cz, investicniweb.cz, ceskapozice.lidovky.cz, patria.cz, openiazoch.zoznam.sk, energetika.tzb-info.cz, cbap.cz, barchart.com,*

BEZPEČNOST FINANČNÍCH INSTITUCÍ

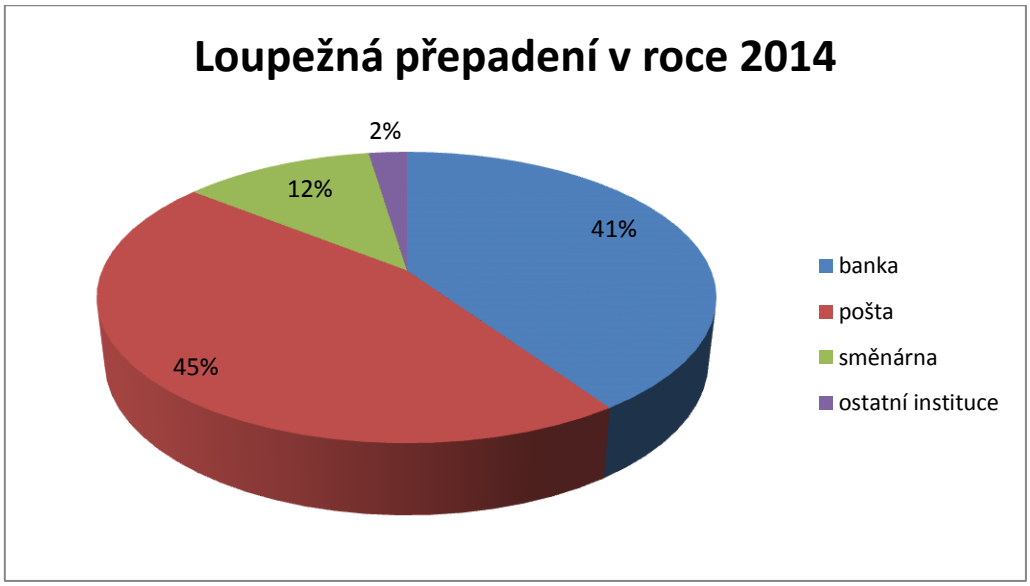
Policejní statistiky a jejich interpretace

Trestná činnost, související s finančními institucemi, je značně rozmanitá a zahrnuje množství skutkových podstat. V této kapitole se nejdříve v policejních statistikách zaměříme na ty nejdramatičtější, a sice **loupežná přepadení**. Následovat budou další formy trestné činnosti od skimmingu až k úvěrovým a pojistným podvodům.

Dobrou zprávou je, že ve srovnání s rokem 2013 **počet loupežných přepadení bank a finančních institucí v České republice výrazně klesl (více než o 50 %**). Zatímco za celý rok 2013 bylo zaznamenáno celkem 88 případů, v roce 2014 pak pouze 42.

Nárůst případů v uplynulých letech byl dáván do souvislosti zejména s ekonomickou krizí a zhoršenou finanční situací řady obyvatel. V minulé situační zprávě jsme vyslovili prognózu, že se v případě zlepšení celkové ekonomické situace a obnovení hospodářského růstu sníží i incidence tohoto negativního společenského jevu. Tento předpoklad se skutečně potvrdil. Svou roli mohou hrát i preventivní opatření. V rámci zlepšování objasněnosti tohoto druhu kriminality je například i nadále prohlubována spolupráce Policie České republiky se členy komise pro fyzickou bezpečnost České bankovní asociace, kdy dochází k pravidelné výměně informací a zkušeností s cílem v co největší míře omezit páchání této trestné činnosti

Nejčastějším terčem lupičů byly v roce 2014 pošty (19 případů), banky následovaly v těsném závěsu se 17 zaznamenanými případy. Směnárny byly v České republice ve sledovaném období přepadeny celkem 5x, z toho 2x v Ústeckém kraji, 2x v Olomouckém kraji a 1x v kraji Královéhradeckém. V roce 2014 byly tedy pošty pro lupiče lákavějším cílem než banky, což je změna oproti situaci v roce 2013, kdy bankovní pobočky poměrně jednoznačně dominovaly. Tehdy se v bankách odehrálo celých 54 % loupežných přepadení, zatímco pošty tvořily jen 27 %.



Z dlouhodobých statistik je zřejmé, že nejčastěji dochází k loupežným přepadením ve velkých městech (Praha, Brno) a dále v regionech se zhoršenou sociální situací. Je pozoruhodné, že jinak velmi výrazná **dominance Prahy** nebyla ve sledovaném období tak patrná, jako v předchozích letech (v metropoli se dříve odehrávala až jedna třetina celkového počtu loupežných přepadení, např. v roce 2013 to bylo 27 %). Případ Prahy je pochopitelně specifický a je dán jejím metropolitním charakterem (velké město přispívá k anonymitě pachatelů, ti také často předpokládají, že zde pobočky bank disponují větší hotovostí).

V roce 2014 zůstala Praha nejrizikovějším městem z hlediska přepadení bank (6 případů, tedy více než třetina z celkového počtu v ČR), **pošty byly ale více ohroženy v kraji Jihomoravském** (pět případů, oproti třem v Praze). Je pozoruhodné, že ani jedna z přepadených směnáren se nenacházela v největších českých a moravských městech (v Praze, Brně, Ostravě, ani Plzni). Loupežných přepadení těchto institucí zůstaly v uplynulém roce ušetřeny 4 kraje: Jihočeský, Pardubický, Karlovarský a Vysočina.

Oproti roku 2013 došlo v uplynulém roce také k výraznému (téměř 50%) poklesu napáchaných škod. **Pachatelé loupežných přepadení si odnesli zhruba 2 255 200 Kč** (oproti více než pěti milionům v roce 2013). Policii se v roce 2014 podařilo odhalit pachatele v 21 případech, tedy přesné polovině všech zaznamenaných. Celková objasněnost tohoto typu kriminality je nicméně vyšší – třebaže některé pachatele se nepodaří dopadnout ve stejném pololetí, kdy zločin spáchali (což se projeví ve statistikách), velice často svůj čin následně opakují, případně jsou odhaleni se zpožděním, takže z dlouhodobého hlediska je úspěšnost policie poměrně vysoká.

Tento typ trestné činnosti nabývá velmi často sériového charakteru – pachatel je mnohdy nadšen počátečním úspěchem a poměrně záhy se pokusí si tímto „snadným“ způsobem vydělat další peníze. V naprosté většině případů tak lupič dříve či později skončí v policejních poutech. Nejčastěji se přitom jedná o lidi, kteří se k tomuto činu zpočátku uchylují kvůli dluhům, které již nejsou schopni splácet. Často se jedná o gamblery, v některých případech i narkomany. Ani úspěšné přepadení banky přitom dluhovou spirálu většinou neukončí, protože pachatelé často získané finance záhy utratí. Většinu přepadení tak tvoří akce amatérů, kteří jsou obvykle v poměrně brzké době dopadeni. Ani vysoký poměr objasněnosti loupeží ze strany policie ale bohužel nevede ke znatelnému úbytku počtu případů, neboť se mnohdy jedná o lidi, kteří možné důsledky svých činů příliš nedomýšlejí. Pokusy profesionálně organizovaných gangů jsou naštěstí poměrně řídké, v těchto případech bývá ovšem zaznamenaná škoda nejvyšší (často mají pachatelé v těchto případech svého „insidera“ přímo mezi zaměstnanci bankovní instituce, případě bezpečnostní agentury).

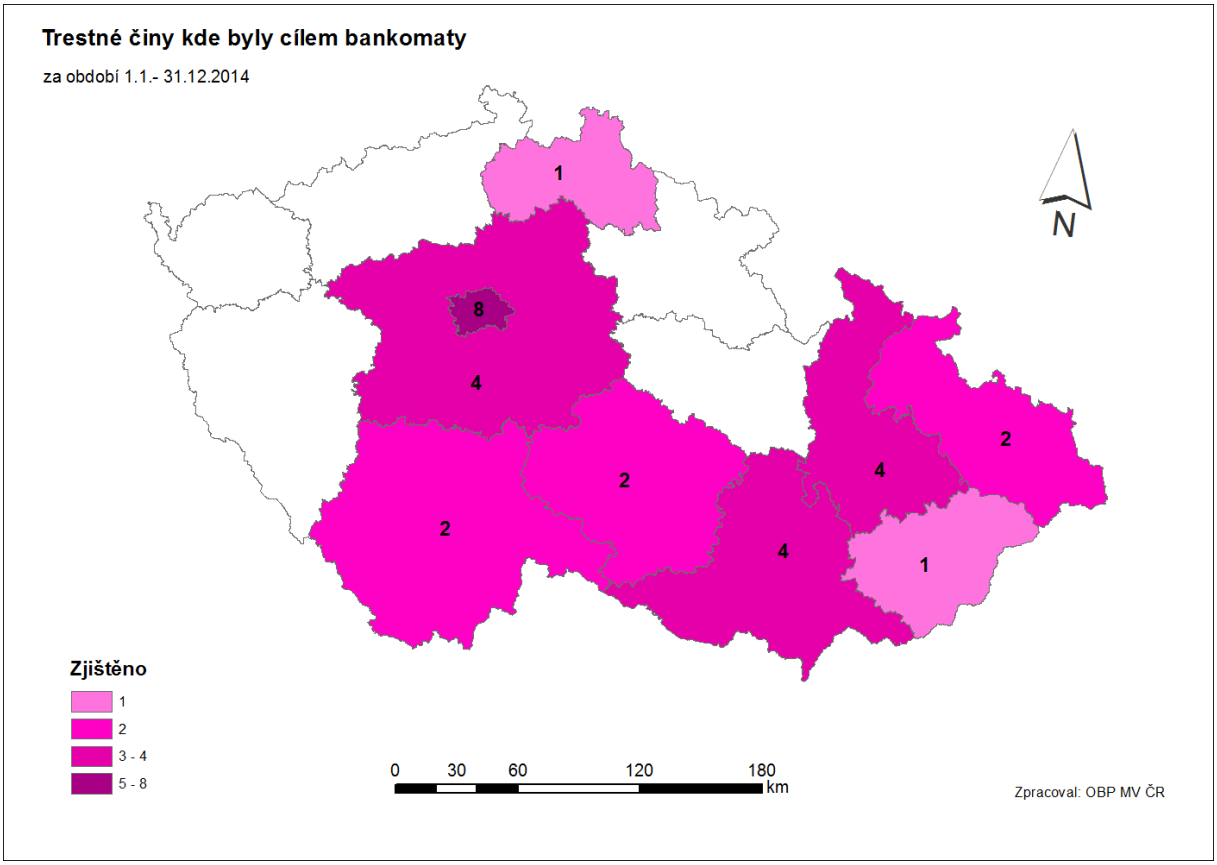
Terčem útoků se ale mnohdy stávají nejen samotné pobočky finančních institucí, ale také jejich zařízení, zejména bankomaty. V druhé polovině roku 2014 registrovala policie **celkem 16 případů, kde byl předmětem zájmu pachatele bankomat**. Škoda přesáhla jeden milion korun, objasněnost byla zhruba čtvrtinová (připomínáme, že řadu pachatelů se daří dopadnout později tj. v jiném pololetí, než ve kterém byl zločin spáchán).

trestné činy, kdy předmětem zájmu byl bankomat
za rok 2014

registrované skutky	28
počet skutků, u nichž byl zjištěn pachatel	8
škoda	4 102 900 Kč

Více polovina z těchto případů byla přitom kvalifikována dle §228 jako poškození cizí věci. Skutková podstata krádeže pak byla naplněna v sedmi případech. Ve dvou případech šlo o neoprávněné opatření, padělání a pozměnění platebních prostředků dle §234.

V této souvislosti můžeme zmínit, že v roce 2014 oslavily bankomaty 25 let svého fungování v České republice. Díky nástupu bezkontaktních platebních karet a stále většímu počtu obchodníků, kteří platbu kartou přijímají, ale nedošlo v loňském roce poprvé za ono čtvrtstoletí k nárůstu celkového počtu výběrů (v roce 2013 jich bylo 183 milionů). Koncem roku 2014 bylo v ČR zhruba 4460 bankomatů, což znamená **průměrnou hustotu 56 bankomatů na jeden kilometr čtvereční** (s pochopitelnou vyšší koncentrací ve velkých městech).



Jak je patrné z mapy, ve sledovaném období došlo k největšímu počtu případů napadení bankomatů v Praze, policie ale obecně registruje stále častější páchání (zejména skimmingu) v regionech, neboť pražská policie se na tento typ trestné činnosti stále více zaměřuje. Vysoký počet případů byl zaznamenán také v Jihomoravském, Olomouckém a Středočeském kraji.

Zřejmě největším problémem pro instituce provozující bankomaty jsou **případy skimmingu**, o jejichž technikách jsme již v předchozích situačních zprávách několikrát informovali. Výjimkou nejsou ani **pokusy o fyzické překonání ochrany bankomatů**. Australská média informovala o kuriózním případu muže ve městě Darwin, který se pár dnů před koncem roku 2014 značně amatérským způsobem pokusil vykrást bankomat s pomocí podomácku vyrobené výbušniny. Výbuch pachatele odmrštil několik metrů daleko a zapálil mu tričko, které si předtím přetáhl přes hlavu, zřejmě aby se vyhnul identifikaci ze záznamu bezpečnostní kamery. Po explozi zjevně otřesený pachatel utekl a neodnesl si z přístroje žádné peníze – jediným výsledkem tak bylo video z jeho nepovedené akce, pořízené bezpečnostní kamerou, které v krátké době dosáhlo celosvětové popularity na sociálních sítích.

Podobný pokus se nicméně v roce 2014 odehrál také v České republice, kde dva muži odpálili výbušninu na bankomatu na pražském sídlišti Skalka. Také tato snaha o krádež neskončila úspěšně – bezpečnostní schránka s penězi zůstala nepoškozena, škoda na přístroji a okolních výlohách ale překročila 600 tisíc korun. Z uvedených případů vyplývá, že výbušniny nejsou pro účely vykrádání bankomatů příliš efektivním nástrojem, naprostá většina úspěšných pokusů tak připadá právě na klasický skimming, který nejen v ČR do značné míry ovládají organizované balkánské gangy.

Ty operují většinou v mezinárodním měřítku a pro jejich dopadení je mnohdy rozhodující spolupráce policejních sborů z různých zemí. Velké úspěchy v tomto ohledu slaví **Evropské centrum informační kriminality (EC3)**, které funguje v Haagu v rámci Europolu. I díky jeho koordinaci se v říjnu 2014 podařil rozsáhlý zásah bulharské a španělské policie proti velké organizované skupině, která se soustředila skimming, podvody s elektronickými platbami a padělání dokumentů. Zatčeno bylo celkem 31 podezřelých, převážně bulharské národnosti (právě bulharské a rumunské gangy v těchto aktivitách v Evropě dominují).

V rámci akce se uskutečnilo přes 40 domovních prohlídek, při kterých byly odhaleny i dvě velmi moderně vybavené laboratoře (v Sofii a v Malaze) pro výrobu zařízení pro skimming a padělání dokumentů, včetně mikrokamer, čteček magnetických proužků a falešných platebních karet. Falešné plastové zdířky a klávesnice, které pachatelé instalovali přímo do bankomatů po celé Evropě (Itálie, Francie, Španělsko, Turecko atd.), byly vyráběny na moderních 3D tiskárnách. Zásahy v obou zemích probíhaly paralelně, což by bez koordinace na evropské úrovni zřejmě nebylo možné.

Centrum EC3 bylo v roce 2014 v koordinaci mezinárodních policejních sil při zásazích proti skimmingovým gangům mimořádně úspěšné. O některých dalších případech jsme informovali již v předchozí situační zprávě. K dalšímu zlepšení by měl přispět podpis **Memoranda o porozumění mezi centrem EC3 a Evropskou bankovní federací**, ke kterému došlo v září 2014 v Haagu. Se stále výraznějším přesunem útoků na bankovní instituce do kybernetického prostoru roste i význam koordinačních a expertních center, jako je právě EC3. Řada bankovních institucí si je tohoto faktu vědoma, a vzájemná spolupráce je tak v tomto ohledu nezbytná. Memorandum umožňuje výměnu důležitých informací, statistik a znalostí mezi oběma stranami. Kooperace s Europolem by tak měla přispět k lepší ochraně evropských finančních institucí – dozvědí se tak rychleji např. o novém malware, nových metodách platebních podvodů atd. Mělo by tak jít o víc, než o pouhé symbolické gesto.

Zatímco skimming se daří pomalu, ale jistě omezovat, útoky na bankovní služby v kybernetickém prostoru mají bohužel i v ČR vzrůstající tendenci. Samotné banky odhadují tento nárůst v desítkách procent ročně. V roce 2014 bylo zaznamenáno velké množství malware a phishingových útoků, které cílily na internetové platby a online bankovní služby. Podle statistiky ČSOB tvoří právě tyto dvě formy útoků naprostou většinu, zbylé využívají sociální sítě (zejména Facebook). Zároveň jsou tyto útoky stále profesionálněji prováděny, takže působí důvěryhodněji.

Časy, kdy se daly např. podvodné emaily snadno rozeznat díky špatné české gramatice (jednalo se většinou o strojové překlady zahraničních phishingových kampaní) jsou do značné míry minulostí – moderním trendem je **sofistikovaný spear phishing**, který cílí na konkrétní osoby (či skupiny osob, např. zaměstnance jedné firmy), o kterých si pachatelé nejdříve zjistí velké množství informací (kupříkladu skrze sociální sítě, firemní internetové prezentace atd.). Tato data pak využijí k formulaci podvodné zprávy, která se může např. tvářit jako email od nadřízeného (včetně jeho skutečného jména a emailové adresy) či spolupracovníka. Drtivá většina napadených v tomto případě nepohlíží na zprávu s podezřením a otevře přiložený soubor se skrytým malware. Podobně na sociální síti Vám zpráva obsahující falešný odkaz může přijít od dobrého přítele (kterému předtím pachatel naboural profil).

V roce 2014 se podvodné zprávy, cílící na zneužití internetového bankovnictví lavinově šířily přes Facebook. Scénář byl obvykle takový, že poškozenému přijde od jeho známého na Facebooku zpráva s prosbou o drobnou finanční výpomoc. Přítel si v ní obvykle stěžuje, že má zablokovanou či nefunkční platební kartu, ale potřebuje rychle provést důležitou platbu v poměrně malé hodnotě (např. 100 Kč). Následoval odkaz na platební bránu, která požadovala buď údaje o platební kartě, případě k přístupu do internetového bankovnictví. Jindy zase přijde (opět od přítele na Facebooku) zpráva, že má problém s telefonem a žádá, zdali by si k vám nemohl přeposlat autorizační SMS s tím, že mu ji následně přepošlete. Pokud to učiníte, můžete se svými penězi rozloučit. Není třeba zdůrazňovat, že váš skutečný přítel ve skutečnosti o ničem neví a je pouze majitelem zkompromitovaného účtu na sociální síti.

Podobně se řada emailových zpráv tváří jako oficiální informace od banky, které oznamují například **expiraci přístupových údajů do vašeho internetového bankovnictví, případně požadují znovu zadat číslo platební karty za účelem obnovy databáze**. Řada lidí v obavě ze zablokování účtu tyto údaje skutečně vyplní. Přiložený aktivní odkaz vyzývá k zadání současných přihlašovacích údajů a hrozí, že v opačném případě bude účet váš zablokován. Věrohodnost takových zpráv umocňuje použití oficiální grafiky vaší banky, kterou ovšem není problém stáhnout z internetu či ji napodobit v běžném grafickém programu. Na tomto místě je nutné zdůraznit, že **banky nikdy nevyžadují přístupové údaje k účtům či čísla platebních karet nebo jejich PIN přes email ani sociální sítě – pokud vám taková žádost přijde, jedná se VŽDY o podvod, bez ohledu na další obsah zprávy**. Podobné je to se žádostmi o přeposlání autorizačních SMS či sdělení autentizačních kódů v nich uvedených. Pakliže máte jakoukoliv pochybnost o pravosti zprávy, můžete si ji u příslušné finanční instituce telefonicky ověřit.

Podle údajů České bankovní asociace **stály právě phishingové útoky za 95 procenty všech neoprávněných čerpání peněz z účtů**. Sama banka v těchto případech nemůže útoku dost dobře zabránit, protože údaje pro provedení platby neunikly z jejího systému, ale pachateli je poskytl díky vlastní neobezřetnosti sám klient. Často mají phishingové útoky např. podobu přání do Nového roku či objednávek zboží z internetových obchodů. Například Česká spořitelna nabízí na svých internetových stránkách https://www.csas.cz/phishing, v sekci "Phishing - tiskové zprávy a aktuality", aktuální přehled probíhajících kybernetických útoků, které cílí na její klienty. Podobná aktuální varování naleznete i na webových stránkách většiny dalších českých bankovních institucí.

Níže je uvedena ukázka falešné stránky, která se po infikování vašeho počítač malwarem může zobrazit přímo v internetovém bankovnictví. Tato stránka vyzývá k instalaci falešné mobilní aplikace „TrustPort Mobile Security“ – cílem hackera je získat, po úspěšném proniknutí do vašeho počítače, také přístup do vašeho mobilního telefonu, což je nezbytné pro překonání dvoufaktorové autorizace pomocí SMS.

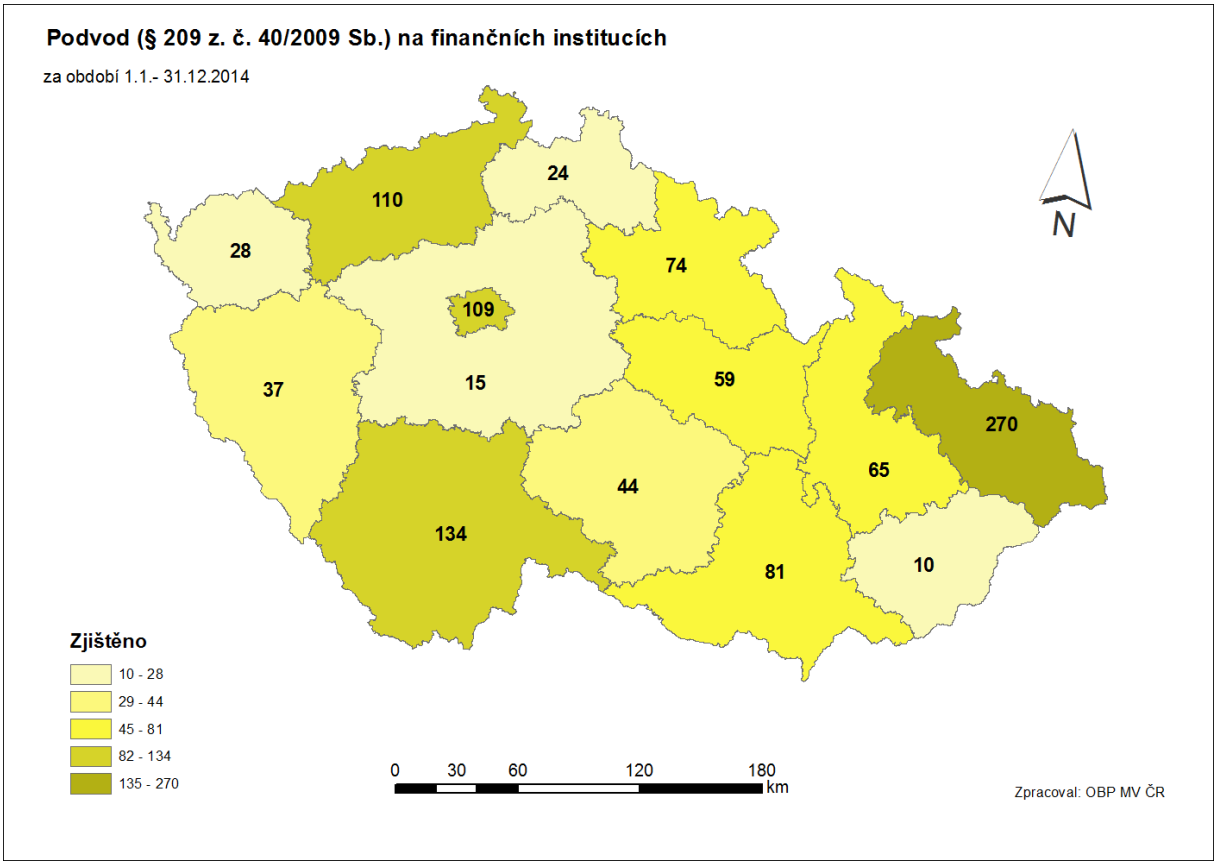
Vůbec nejúspěšnější jsou takové útoky, které v napadeném vyvolají obavu (např. z dluhu či zanedbání nějaké povinnosti), případně takové, které nabízejí aktualizaci či posílení zabezpečení. Často tak dochází k paradoxní situaci, kdy si uživatel v dobré víře, že tím zlepšuje ochranu svého zařízení, sám instaluje nebezpečný virus. Do první manipulativní kategorie patřila série emailů z druhé poloviny roku 2014, která se **vydávala za zprávy od Exekutorské komory**. Mnozí lidé se z obavy z exekuce skutečně pokoušeli dluh zaplatit. Někdy email požaduje přímou platbu, jindy se pouze pokouší získat přístup do internetového bankovnictví či k číslu platební karty. Kvůli tomuto spamu se na Exekutorskou komoru postupně obrátilo 17 tisíc Čechů. Emaily totiž působily velmi reálně a přesně v duchu kvalitního spear phishingu obsahovaly dokonce pravá jména skutečných exekutorů. Netřeba dodávat, že ani Exekutorská komora nevymáhá dluhy prostřednictvím emailu.

Na závěr kapitoly přinášíme opět statistiky různých forem podvodů podle §209 Trestního zákoníku, který si pro přehlednost zúžíme pouze na objekt hospodářské kriminality (a pomineme kriminalitu obecnou). Počet těchto skutků přehledně znázorňuje následující tabulka:

podvod (§ 209 z. č. 40/2009 Sb.) na finančních institucích
objekt hospodářské kriminality za rok 2014

registrované skutky	1060
počet skutků, u nichž byl zjištěn pachatel	813
škoda	152 494 200 Kč

Ve srovnání s prvním pololetím roku 2014 byla ve druhém pololetí obdobná incidence těchto skutků, výrazně ale poklesl objem napáchaných škod. Z tabulky je zřejmé, že objasněnost těchto případů ze strany Policie ČR je vysoká, pachatele se podařilo odhalit ve více než třech čtvrtinách případů. Co se týče geografického rozložení, pak se v tomto případě jedná o jeden z mála sledovaných trestných činů, ve kterém nevévodí Praha. Ta je se 109 spáchanými skutky dokonce až na čtvrtém místě a překonávají ji kraje Moravskoslezský (270 případů), Jihočeský (134 případů) a Ústecký (110 případů). Nejméně podvodů bylo zaznamenáno ve Zlínském kraji a ve středních Čechách.



Pokud se dále zaměříme na problematiku **úvěrového podvodu** (§211), získáme následující čísla:

úvěrový podvod (§ 211 z. č. 40/2009 Sb.) na finančních institucích objekt hospodářské kriminality za rok 2014

registrované skutky	3124
počet skutků, u nichž byl zjištěn pachatel	2 592
škoda	1 009 096 600 Kč

Také objasněnost úvěrových podvodů je značně vysoká (83%), škody v této oblasti nicméně v loňském roce přesáhly jednu miliardu korun. Tento typ trestné činnosti je nejrozšířenější v Jihočeském kraji (491 případů), v Praze (481 případů) a v Moravskoslezském kraji (433 případů). Naopak nejlépe je na tom opět kraj Zlínský.

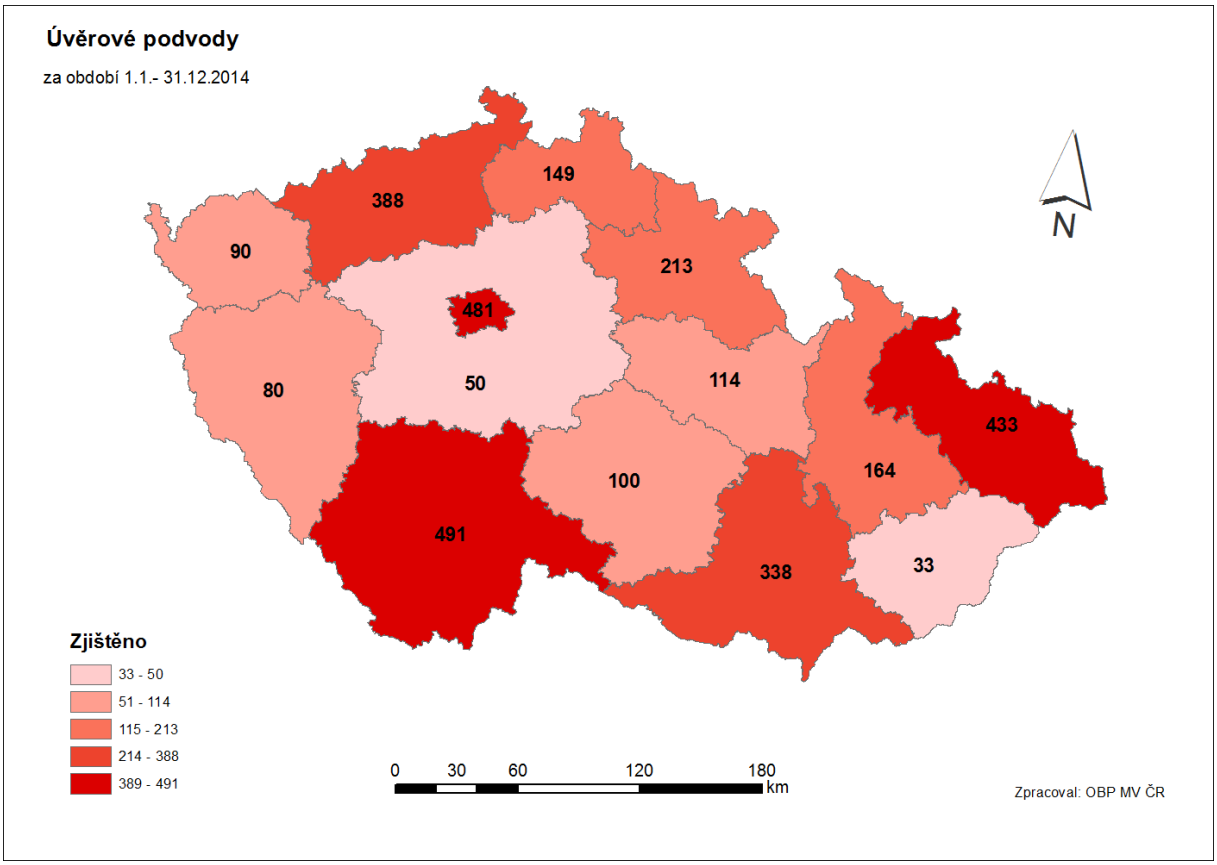
Z výše uvedeného je patrné, že **úvěrové podvody** zůstávají v České republice dosti rozšířené. Alarmující je zejména fakt, že se o takové podvody **často pokoušejí i lidé, kteří mají čistý trestní rejstřík** – takových byla z celkového počtu zaznamenaných případů téměř polovina, což je u jiných typů kriminality neobvyklé (jinde často převažují recidivisté). Řada lidí má pocit, že může tímto způsobem velmi snadno získat peníze, a že k tomu stačí poměrně snadno padělatelné dokumenty (např. výpisy z účtů, potvrzení o příjmu či zaměstnání atd.), či např. vyfabulovaný úžasný podnikatelský projekt.

Zejména spotřebitelské úvěry a nákupy na dluh poskytují (především nebankovní společnosti) skutečně masově a často s minimálním ověřováním schopnosti budoucího dlužníka splácet. U některých lidí to vyvolá mylný dojem, že se tímto způsobem mohou beztrestně obohatit. Ale pozor, pokud přestanete úvěr splácet, podvod bývá velmi rychle odhalen a i v případě původně nízkých částek hrozí několikaleté vězení. **Úspěšnost objasňování Policie ČR se u úvěrových podvodů pohybuje nad 80%, naprostá většina podvodníků tak na svůj pokus doplatí**.

Příkladem může být jednadvacetiletý mladík z Horního Slavkova, který si přes internet, na základě údajů z občanského průkazu svého kamaráda, půjčil 3 000 Kč. Do té doby bezúhonný mladík půjčku na účet skutečně dostal, jeho podvod byl ale velmi rychle odhalen. Byl obviněn nejen z úvěrového podvodu, ale také (vzhledem ke zneužité cizí občance) z poškození cizích práv, za což mu hrozilo až 2 roky vězení nepodmíněně. Mladý pachatel byl velmi překvapen tím, jak vysoký trest mu hrozí za pouhé tři tisícovky. V těchto případech navíc samozřejmě není ani vrácení peněz důvodem k zastavení obvinění, neboť tím se může vypořádat dluh vůči bance, nikoliv však vzít zpět již uskutečněný trestný čin (použití falešných dokladů, a tedy podvod při získání úvěru).

Někteří zkušenější pachatelé, například muž a žena z Písku, si nicméně na úvěrových podvodech dokázali založit živobytí. Policie jim jich prokázala hned dvanáct, v celkové hodnotě 1,4 milionu korun. Obohacovat se tímto způsobem se jim dařilo šest let. Takové případy dlouho unikajících pachatelů jsou ale spíše výjimkou. Nejčastěji se spotřebitelského úvěru dopouštějí „obyčejní“ lidé, kteří nedomyslí důsledky svého jednání a domnívají se, že jejich podvodný plán nikdo neodhalí. To může být případ sedmdesátiletých manželů z Prachaticka, kteří falšovali údaje o svých příjmech a na několika spotřebitelských úvěrech vyinkasovali 130 tisíc korun. Jiným typickým případem z loňského roku byl nezaměstnaný muž z Velkých Losin, který si v bance v Šumperku pokusil půjčit 400 tisíc korun, přičemž předložil padělaný doklad o měsíčním příjmu 37 tisíc Kč.

Ačkoliv by se tedy zdálo, že úvěrový podvod je rychlá cesta k penězům, ve skutečnosti se jedná více o spolehlivý způsob, jak si zničit život. Je totiž nutné zdůraznit, že se o podvod jedná (a trest odnětí svobody a zápis v trestním rejstříku vám hrozí) i v případě, že podvodně získaný úvěr splácíte – stačí při jeho získávání předložit padělané dokumenty či doklady. Vzhledem k počtu objasněných případů je pokus o úvěrový podvod jedním z nejhloupějších možných začátků kriminální dráhy.



V rámci problematiky **pojistných podvodů** jsou stále zaznamenávány jako nejčetnější podvody v souvislosti s pojištěním vozidel, nicméně stejně jako v roce 2013 jsou na vzestupu pojistné podvody v souvislosti s pojištěním osob. Jejich zjišťování a objasňování však patří mezi ty složitější, a proto je na místě i v roce 2015 věnovat větší pozornost těmto formám páchání trestné činnosti.

Závěrečná tabulka shrnuje přehled trestných činů, kde se objektem hospodářské politiky stala v roce 2014 pojišťovna.

trestné činy, kdy objektem hospodářské kriminality byla pojišťovna za období leden až prosinec 2014

	§ 206 Zpronevěra	§ 209 Podvod	§ 210 Pojistný podvod	§ 211 Úvěrový podvod	§ 220 Porušení povinnosti při správě cizího majetku	§ 230 Neopr. přístup k počít. syst. a nosiči inf.	§ 241 Neodved. daně, pojist. na soc. zabezp.	§ 254 Zkreslování údajů o stavu hospodaření a jmění
registrované skutky	18	73	344	3	2	2	151	1
počet skutků, u nichž byl zjištěn pachatel	11	52	231	1	1	0	136	1
škoda	41 449 100 Kč	25 600 500 Kč	103 158 300 Kč	300 000 Kč	0 Kč	0 Kč	20 584 300 Kč	1 368 000 Kč

Exkurz: Vícefaktorová autorizace a využití biometriky

Historie internetového bankovnictví sahá podle některých autorů až do roku 1982. Dlouho byly tyto služby chráněny pouze jednoduchými hesly. Ochrana internetového placení pomocí pouhého **přístupového jména a hesla** (případně PINu), **se v době rozšiřujících se kybernetických útoků stává stále nedostatečnější**. Řada bank tak (zejména u rizikových klientů) přistupuje k dalším **doplňkovým formám autorizace**, které ztěžují případné zneužití daného účtu.

Mezi nejběžněji používané patří běžná **autentizační SMS**. Banka zašle na registrovaný mobilní telefon autentizační kód, ten uživatel ručně přepíše do určeného pole v internetovém bankovnictví, čímž autorizuje příslušnou finanční operaci. Technický pokrok učinil tuto metodu paradoxně zranitelnější, než byla dříve – na rozdíl od původních mobilních přístrojů jsou totiž současné smart phony v podstatě přenosnými počítači a jakožto počítače jsou také náchylné k nákaze malware či ke kybernetickému útoku. Nízká pozornost, kterou mnozí uživatelé věnují zabezpečení svého mobilního zařízení, tyto útoky výrazně usnadňuje. Z výsledků ankety společností AVG a Ponemon Institute vyplývá, že **pouze 29% vlastníků mobilních telefonů má na svém přístroji nainstalovaný antivirový program** (ať již placený či neplacený), anebo jeho instalaci alespoň zvažuje. To je dost alarmující číslo, které je velmi pozoruhodné i v tom ohledu, že v případě klasických PC je počet zařízení vybavených nějakým antivirovým softwarem podle odhadů přes 80% (podle zprávy McAfee to bylo celosvětově 83% v roce 2012, poměr vůči mobilním telefonům je tedy velmi znatelný).

Staré telefony z 90. let byly vzhledem k absenci pokročilého operačního systému vůči kybernetickým útokům výrazně odolnější. V roce 2014 se tak objevila řada podvodných kampaní a počítačových virů, které (většinou metodou phishingu) cílí na překonání autorizace prostřednictvím klasické SMS. Následují tak cestu malwaru Eurograbber, jednoho z nejúspěšnějších virů vůbec, který, skrze paralelní napadení internetového bankovnictví v PC a mobilního telefonu, dokázal z účtů po celé Evropě vysát v přepočtu několik miliard korun. Některé banky nabízejí v tomto ohledu vyšší ochranu ve formě **šifrovaných autentizačních SMS**, které lze použít jen v kombinaci s příslušnou kryptografickou aplikací. Ani tato metoda nemusí být při kompromitaci či ztrátě telefonu stoprocentně bezpečná.

Pro vybrané klienty banky stále nabízejí službu **autentizačního kalkulátoru**, tedy malého přístroje, který automaticky vygeneruje jedinečný kód pro danou transakci. Tento systém je obecně poměrně bezpečný, zejména proto, že jej využívá poměrně malé množství lidí (často se jedná o korporátní klienty). Jeho nevýhodou je totiž nutnost nosit při sobě stále další přístroj, služba je navíc často za příplatek. Pro zvýšení uživatelského komfortu fungují nově jako autentizační kalkulátory také některé platební karty, které mají vlastní displej, na kterém se kód zobrazí. Ani ty ale zatím nejsou příliš rozšířené.

Dalším způsobem ochrany je stvrzování bankovních operací **podpisovým certifikátem**, což je vlastně heslem chráněný šifrovaný soubor, který je uložen na disku v počítači, na přenosovém disku, případně optické či čipové kartě (v tom případě uživatel potřebuje čtečku čipových karet). Někdy je podpisový certifikát uložen na speciálním USB tokenu. Ještě méně využívané jsou tzv. **TAN kódy**, jejichž seznam banka předem pošle např. klasickou poštou. Tento kód tvoří unikátní, zpravidla 6místné číslo, kterým se potvrdí bankovní operace. Po potvrzení je TAN kód neplatný a je potřeba příště použít jiný.

V každém případě je výhodné **používat alespoň jednu další formu autentizace** (i klasická autorizační SMS výrazně zvyšuje bezpečnost vašeho internetového bankovnictví) a nespoléhat se pouze na zabezpečení uživatelským jménem a heslem. Tvorbě hesla je třeba také věnovat patřičnou pozornost a řídit se pravidly pro vytvoření tzv. silného hesla (počet znaků atd.). V současné době se banky snaží vypořádat s novými zákaznickými trendy, tedy zejména rostoucím zájmem lidí o mobilní přístup ke svému účtu, odkudkoliv, kdekoliv a z různých zařízení. Přitom je potřeba upozornit, že mobilní zařízení jsou obecně vnímána jako rizikovější (jak jsme již upozorňovali v předchozích situačních zprávách).

Dnešní útoky jsou v zásadě mnohem sofistikovanější a profesionálněji prováděné, než tomu bylo ještě před několika málo lety. Běžné jsou dnes **útoky multivektorové**, které kombinují více kanálů a typů ataku (např. zavirovaný email a webový exploit). Často se jedná o několik zdánlivě nezávislých kroků, které si uživatel vzájemně nespojí. Velmi časté jsou falešné formuláře, které se čím dál více podobají originální grafice banky (občas se liší např. mírným překlepem v adresním řádku, kterého si ale málokdo všimne, moderní malware dokonce dokáže zakrýt i tento drobný indikátor potenciálního problému).

Tři nejúspěšnější současné malware, které cílí také na banky, jsou: **Zeus** (jeden z prvních pokročilých malware, vyskytuje se i v mobilní verzi); **Spye Eye** (modernější varianta malwaru Zeus) a nejnovější **Citadel** (velmi sofistikovaná, šifruje komunikaci zařízení s útočníkem, takže je téměř neodhalitelná, dokáže udělat např. video obrazovky uživatele, takže útočník přesně vidí, co dělá atd.).

V České republice byla od roku 2013 hodně rozšířená varianta malwaru Zeus zvaná **Hesperbot**, která kombinovala phishingový email s infikovanou pdf přílohou, díky které získal útočník kontrolu nad prohlížečem. Útočníci měli zaregistrovanou doménu „ceskaposta.net“ (skutečná je „ceskaposta.cz“), kam napadený prohlížeč uživatele automaticky přesměrovával. Malware také uměl při přístupu na falešné stránky potlačit ověřování certifikátů. Hesperbot měl také velmi kvalitně provedenou mobilní verzi (dokonce různé verze pro různé platformy – Android, Blackberry atd.). Uživateli se pak nabídla falešná bezpečnostní aktualizace, kterou byl vyzván k zadání bezpečnostního kódu. Ten byl ve skutečnosti kódem k autorizaci platební transakce.

Vyrobit jednoduchý malware přitom není vůbec problém a může si jej pořídit kdokoliv – už za ceny od 100 dolarů výše vám **anonymní hacker vyrobí malware** přesně dle vaší objednávky a dodá **„na klíč“**, takže ani nemusíte mít žádné IT znalosti. V České republice je mobilní bankovnictví velkým hitem a lidé mu dávají stále větší přednost. Češi se také čím dál častěji podepisují elektronickým podpisem (ten je přitom zneužitelný a při nedodržení bezpečnostních pravidel se dá znovu použít na úplně jiný dokument).

Celý proces autentizace slouží primárně k ověření toho, že transakci provádí skutečně klient, a ne někdo jiný. V současné době jsou proto trendem moderní metody, které se snaží hesla a kódy nahradit lepší znalostí konkrétního uživatele. Velké možnosti v tomto směru nabízí **behaviometrika**, která se snaží podle způsobu chování (např. způsobu zadávání hesla, rychlosti spojování bodů při odemykání telefonu atd.) rozpoznat, zda se jedná o původního uživatele, anebo o cizí osobu, která jen drží v ruce jeho telefon. Pokud systém vyhodnotí rizikové chování, uživateli transakci nepovolí, případně bude vyžadovat dodatečnou autentifikaci (např. další heslo, případně operátor uživateli přímo zavolá, aby si ověřil, že je to skutečně on). Čím častěji uživatel systém používá, tím jsou behaviometrické výstupy přesnější a spolehlivější.

Společně s behaviometrikou moderní systémy využívají kombinace dalších zjistitelných údajů k vyhodnocení rizikovosti transakce, která souvisí s historií uživatele a jeho běžným chováním (uživatel se např. najednou přihlašuje z netradičního místa, z jiného zařízení, změnil připojení z klasického na VPN atd.). Systém sám ze všech dostupných údajů vyhodnotí rizikovost operace a doporučí případnou dodatečnou autentizaci.

Ke slovu také stále častěji hlásí **biometrie**, tedy metoda založená na rozpoznávání jedinečných biologických charakteristik (morfologických, fyziologických) každé osoby, které jsou pro každého živého člověka jedinečné a neměnitelné. Může se přitom jednat o otisky prstů, rozpoznání oční duhovky atd. Například polská banka BPS jako první instituce tohoto druhu Evropě zprovoznila bankomat, kde se po vložení karty namísto zadání PINu používá **otisk prstu**. Systém se již běžně používá v Japonsku, do Evropy dorazil až v nedávné době. Zákazník se k této speciální službě musí zaregistrovat a nechat si otisk v bance sejmout. BNS plánuje nainstalovat asi 200 takto vybavených bankomatů.

Společnost MasterCard představila v říjnu 2014 první bezkontaktní platební kartu na světě, která se ověřuje pomocí otisků prstů. Obsahuje integrované biometrické čidlo a zabezpečenou biometrickou technologii autentizace Zwipe, jež uchovává biometrická data držitele karty. Údaje o otiscích prstů jsou tak uloženy přímo na kartě, nikoli v externí databázi. Tuto novinku již úspěšně testovala norská banka Sparebanken DIN. Zwipe nyní připravuje příští generaci karty, která bude mít stejný formát jako standardní karta a bude fungovat se všemi platebními terminály. Na trh by měla být uvedena v roce 2015. Nová karta bude čerpat energii z platebních terminálů, a nebude tedy vyžadovat baterii.

Jelikož se objevily některé metody, které spolehlivost otisků prstů (např. při odemykání mobilních telefonů) zpochybňují, společnost Fujitsu představila v roce 2014 ještě průlomovější techniku, která spočívá ve **snímání mapy krevního řečiště v dlani**. Také tu má každý člověk jedinečnou, navíc ji nelze tak snadno zkopírovat. Technologie PalmSecure je určena pro finanční systémy (např. bankomaty), zabezpečení armádních, vládních nebo firemních počítačů. Na letošním veletrhu CeBIT výrobce ukázal první ultrabook, který má tuto čtečku zabudovanou přímo v těle. Autentizace trvá méně než vteřinu, stačí přiložit dlaň nad snímač. Teoreticky by se tak mohlo jednat o průlomové opatření v boji (nejen) se skimmingem.

Tuto novou technologii si budou moct příští rok vyzkoušet vybraní klienti britské banky Barclays, uvažují o ní i české bankovní domy. Některé již využívají či testují také autentizaci podle hlasu. **Kombinace biometrie a behaviometriky může představovat budoucnost zabezpečení platebních prostředků** a v tuto chvíli se zdá jen obtížně prolomitelná ze strany potencionálních útočníků. Její skutečné zranitelnosti ale jako vždy ukáže až čas.

Vybrané události ve sledovaném období

Červenec

Policisté varovali před další vlnou podvodných mailů

Krajské ředitelství policie Ústeckého kraje zaznamenalo již čtvrtou vlnu, kdy lidé obdrželi nevyžádaný podvodný mail s výzvou k uhrazení smyšleného dluhu. Přílohou toho mailu byl soubor ve formátu ZIP, kdy po jeho otevření došlo k zavirování počítače. Příloha obsahuje smyšlenou smlouvu. Provedeným šetřením bylo zjištěno, že po stažení uvedeného viru získává útočník plnou kontrolu nad počítačem.

V červenci 2014 se na policii v celé České republice obraceli lidé, kterým byly prostřednictvím internetového bankovnictví neoprávněně převedeny značné finanční částky. Je zadokumentován případ, kdy občan obdržel zmiňovaný podvodný e-mail a otevřel přílohu. Dále při přihlášení do svého internetového bankovnictví, (kde vyplnil login a heslo) a čekal na potvrzovací SMS, tato již nepřišla. Místo toho se otevřelo nové okno prohlížeče a stránky se jevily jako stránky příslušné bankovní instituce. Zde byl uživatel vyzván k potvrzení instalace aplikace, která mu byla následně zaslána na mobilní telefon. Po stažení aplikace do mobilního telefonu a vygenerování kódu vložil tento kód do internetového bankovnictví. Tímto útočník získal plnou kontrolu nad bankovním účtem a došlo k převodu finančních prostředků.

Lupič se v bance ve Frýdku – Místku maskoval ženskou parukou

7. července 2014, krátce po třetí hodině odpoledne vešel do komerční banky ve Frýdku-Místku muž, který požadoval peníze pod pohrůžkou útoku bombou. Asi pětadvacetiletý mladík, štíhlé postavy s krátce střiženou bradkou, vešel do haly banky jako standardní klient. Vyzvedl si pořadové číslo a čekal, až přijde na řadu. Takřka normální obrázek, až na to, že od pohledu normální muž měl na hlavě dámskou paruku. Když přišel na řadu, přistoupil k přepážce, položil na pult igelitovou tašku a dopis, ve kterém mladík sděloval, že v přiložené igelitové tašce je výbušnina. Beze slova pak místo a samotnou banku opustil.

Pracovnice banky ihned kontaktovala policii. Policejní hlídka místo zajistila a celou budovu, ve které se nacházelo bezmála padesát osob, evakuovala. Přizvaný pyrotechnik zjistil, že se v igelitové tašce nenachází žádný nástražný výbušný systém, ale pouze kámen. Samotný dopis pak obsahoval výhružku, že pokud mu nebudou doručeny peníze na smluvené místo, tak bomba v tašce vybuchne. Opatření a částečná uzávěra s omezením dopravy okolo místa události trvaly do deváté hodiny večer. Muži v paruce za jeho jednání, které je kvalifikováno jako zločin loupeže, hrozí nepodmíněný trest, a může tak za mřížemi strávit až deset let.

Srpen

Útok na data Evropské centrální banky

Evropská centrální banka se stala terčem crackerského útoku. Její vedení oznámilo, že útočníci pronikli do databáze obsluhující její web a ukradli e-mailové adresy a další kontakty lidí, kteří se zúčastnili akcí pořádaných bankou. Banka ubezpečila, že data, která by mohla ovlivnit vývoj na trzích, ovlivněna nebyla. V případě odcizených dat se jedná o nešifrované části databáze, kde jsou například e-mailové adresy, telefonní čísla a fyzické adresy kontaktů ECB. Jde především o kontakty na lidi, které banka zve například na konference – tato databáze je fyzicky oddělena od dalších systémů. Banka se o úniku kontaktních informací dozvěděla až poté, co jí přišel anonymní e-mail požadující peníze za navrácení dat.

Září

Nová hůře padělatelná desetieurovka je už v oběhu

V minulé situační zprávě jsme informovali o připravovaném posílení bezpečnostních prvků u desetieurových bankovek. V září 2014 se tato nová bankovka ze série Europa dostala do oběhu. Nové bankovky mají několik zdokonalených ochranných prvků a nový nátěr, díky němuž mají být odolnější. Na hologramu a vodoznaku je podobizna bájné řecké princezny Európy, která dala název bankovce i celému kontinentu. Z dalších bezpečnostních prvků natištěná číselná hodnota na přední straně při naklonění bankovky mění barvu od smaragdově zelené po tmavě modrou a při naklonění vytváří lesklé číslo světelný efekt. Na obou krajích přední strany bankovky je také nový druh rýhování.
Nové bezpečnostní prvky na bankovkách mají ztížit práci padělatelům. Loni ECB stáhla z oběhu 670 tisíc falešných bankovek. Meziročně se tento počet zvýšil o více než čtvrtinu. Nejvíce se falšují bankovky v hodnotě 20 a 50 eur. V oběhu je celkem více než 15 miliard bankovek. Právě nová dvacetieurová bankovka má přijít na řadu v roce 2015, nová pětieurovka je v oběhu již od května 2013. Dosavadní desetieurové bankovky zůstávají i nadále v platnosti. ECB je bude stahovat z oběhu později.

Ozbrojení policisté přišli do banky zajistit peníze z trestné činnosti

V souvislosti s kauzou firmy Edbusy zasahovali v září 2014 policisté protikorupčního útvaru v pražské a brněnské pobočce banky Oberbank. Podvodníci z firmy Edbusy slibovali v letech 2007 až 2009 sjednání půjčky za velmi výhodných podmínek a vybírali od důvěřivých lidí zálohy za zprostředkování ve výši několika tisíc korun. Dva lidé za to byli odsouzení na 8,5 a 8 let vězení, čtyři další obžalovaní na rozsudek stále čekají. Pachatelům se podařilo obelhat více než dvanáct tisíc klientů a připravit je o více než 550 milionů korun. Díky zásahu Policie ČR mají oběti firmy šanci na získání zpět další části peněz.
Krajský soud v Brně již v roce 2012 přiznal poškozeným nárok na vyplacení alespoň částečné náhrady, jedna z bank (Oberbank) ale přes závazné soudní rozhodnutí odmítala zajištěné výnosy z trestné činnosti převést na depozitní účet soudu. Ozbrojení policisté proto na pobočkách zabavili požadovaných 93 milionů korun v hotovosti.

Říjen

Lupiči z Děčínska odešli od soudu s vysokými tresty

Krajský soud v Ústí nad Labem vynesl rozsudek v procesu s lupiči, kteří přepadli dvě bankovní pobočky, jednu ústeckou hernu a řadu čerpacích stanic. Hlavní organizátor Jaroslav Kubička dostal 10 let vězení a státu propadlo auto, které si z lupu pořídil. Celkem se mu podařilo prokázat škodu 760 tisíc Kč. Druhý obžalovaný byl odsouzen na šest let a byla mu nařízena protialkoholní léčba. Dva další, spolupracující obviněné, poslal soud do vězení na čtyři roky. U soudu stála i jedna žena, přítelkyně jednoho z obžalovaných, která o loupežných útocích věděla. Tu trestní senát odsoudil na jeden rok s dvouletou podmínkou.

Z bankomatu ve Štěchovicích byly uloupeny statisíce korun

Pachatelé přepadli pracovníka bezpečnostní agentury, který právě prováděl servis přístroje. Loupež se obešla bez zranění, pachatelé z místa utekli. Bankomat předtím zřejmě pachatelé sami poškodili, aby si vynutili příjezd obsluhy. Na místo vyrazili hlídky operačního odboru Policie ČR, výjezdové skupiny Služby kriminální policie a vyšetřování i vrtulník letecké služby PČR. Policisté prověřovali i verzi, že si pracovník agentury celé přepadení vymyslel (ve skutečnosti je totiž fiktivních až 40% nahlášených loupeží). Nakonec se ale ukázalo, že to není tento případ. Policisté totiž skutečného pachatele dopadli už

po 62 hodinách v Praze a byla na něj uvalena vazba. U muže byla nalezena krátká střelná zbraň a také uloupené peníze. Hrozí mu až deset let vězení.

Listopad

Zásah českých a německých policistů proti padělatelům dolarů

Němečtí a čeští policisté a státní zástupci zasáhli proti přeshraniční skupině, podezřelé z padělání peněz. Na začátku roku 2014 byla detektivy Útvaru pro odhalování organizovaného zločinu SKPV zjištěna z kriminálního prostředí informace, že se osoby z Libereckého a Ústeckého kraje snaží vytvořit distribuční kanál na vývoz padělaných bankovek, které jsou vyráběny v padělatelské dílně na území Spolkové republiky Německo. Bankovky měly být určeny pro vývoz do třetích zemí (Ukrajina, Pobaltské státy). O spolupráci byly požádány prostřednictvím německého styčného důstojníka v Praze specializované policejní jednotky ze SRN.

V únoru 2014 byly v ČR zahájeny úkony trestního řízení, dozorovaného Krajským státním zastupitelstvím v Ústí nad Labem, pobočka Liberec. Prostřednictvím Nejvyššího státního zastupitelství v Brně bylo požádáno o vytvoření společného vyšetřovacího týmu. Tento tým, logisticky podporovaný Eurojustem, vytvořili zástupci policie a justice ČR, zástupci saské policie a státního zastupitelství Görlitz. Cílem společného vyšetřovacího týmu bylo identifikovat konkrétní pachatele, narušit jejich činnost a shromažďovat a sdílet relevantní informace a důkazy pro účely trestního stíhání a konfiskace zisků v SRN nebo ČR.

V průběhu prověřování se potvrdilo, že se na území České republiky pachatelé snaží vytvořit nový distribuční kanál pro převoz padělaných amerických dolarů, který by v budoucnu mohl sloužit i pro převoz drog ze SRN do dalších zemí Evropské unie. Detektivům ÚOOZ SKPV se podařilo začátkem října v severních Čechách zajistit první zásilku padělků v hodnotě 50.000 USD. Za zmínku stojí, že za tuto zajištěnou zásilku požadovali pachatelé částku 12.000 euro. Šetřením společného vyšetřovacího týmu byly identifikovány všechny podezřelé osoby, které se měly na výrobě padělaných bankovek a jejich následné distribuci podílet. Většina podezřelých měla bohatou trestní minulost a systém policejní práce jim tak byl dobře znám. Ke komunikaci používali moderní komunikační technologie a vzájemné osobní schůzky na předem vytipovaných místech.

Hlavním organizátorem měl být podle detektivů pětapadesátiletý občan ČR z Ústí nad Labem. Právě on měl zajistit vybudování nové kurýrní cesty do východoevropských států, kde je v kriminálním prostředí o padělané americké dolary značný zájem. Padělky pak měl naopak vyrábět v německém Zittau pětašedesátiletý občan SRN. Ke společné koordinované akci českých a německých detektivů došlo 17. listopadu 2014. Dvě podezřelé osoby, pětapadesátiletý občan ČR a o pět let mladší občan SRN, byly zadrženy ve spolupráci s Útvarem rychlého nasazení v odpoledních hodinách v Děčíně a Ústí nad Labem, po předání další zásilky padělků v hodnotě 100.000 USD, která byla připravena k distribuci. Ve stejný den došlo k zadržení dalších dvou osob na území Spolkové republiky Německo.

V rámci 12 domovních prohlídek a prohlídek jiných prostor, které proběhly na území ČR, SRN a v Polsku, byla v Zittau zajištěna kompletní padělatelská dílna. V té byly nalezeny všechny komponenty potřebné pro výrobu padělaných bankovek (tiskařské barvy, kopírovací přístroje, tiskařské desky, speciální barvy a roztoky pro tisk, počítačová technika). V dílně bylo také nalezeno větší množství padělaných amerických dolarů určených pro další zásilku. Tyto padělky byly znalci z České národní banky ohodnoceny na stupnici nebezpečnosti 2 (nebezpečné) a 3 (zdařilé), tedy při běžném styku s bankovkou velmi těžko odhalitelné. Dále bylo zajištěno i větší množství anabolik a pyrotechnického materiálu. Zajištěna byla rovněž luxusní zahraniční vozidla v hodnotě několika milionů korun, která měli členové skupiny při trestné činnosti používat.

Oba muži, zadržení v ČR, byli obviněni ze zvlášť závažného zločinu padělání a pozměnění peněz. Okresním soudem v Liberci byli následně vzati do vazby. V případě prokázání viny jim hrozí 5 až 10 let odnětí svobody. V rámci trestní řízení, které současně probíhá i v SRN, byla obviněna jedna osoba (65), které hrozí úhrnný trest od 2 do 15 let.

Prosinec

V Chropyni hořel bankomat
V noci na 9. prosince 2014 byl hasičům v Chropyni na Kroměřížsku nahlášen požár bankomatu na náměstí Svobody. Intenzita zamoření kouřem byla tak vysoká, že hasiči museli při likvidaci požáru použít dýchací zařízení. Škoda byla vyčíslena na 1,2 milionu korun. Příčina vzplanutí zatím není známá.

Anonymous zveřejnili na internetu data tisíců kreditních karet
Zloději dat, hlásící se k hackerskému hnutí Anonymous, zveřejnili na internetu seznam více než 13 tisíc platebních karet, včetně jejich bezpečnostních prvků. Ty tak mohl kdokoliv zneužít ke krádeži finančních prostředků z účtů majitelů karet. Data získali hackeři, podle svých prohlášení na Twitteru, během několika útoků na různé společnosti (např. Amazon, Dell, Walmart, EA Games), kterým jejich zákazníci platí za zboží a služby kreditními kartami (data tedy neunikla z bankovních systémů či databází výrobců kreditních karet).
Na seznamu jsou kromě čísel karet také údaje o konci platnosti a bezpečnostní kódy, tedy vše, co je potřeba znát pro uskutečnění internetové platby. Není vyloučeno, že některé karty patřily také českým uživatelům. Banky a výrobci kreditních karet po zveřejnění seznamu problematické kreditky zablokovali, upozornili zároveň na to, že řada údajů byla již neaktuálních (hackeři je sbírali delší dobu) či nesprávných.

Soud poslal vůdce lupičské bandy na 12 let do vězení
Olomoucký vrchní soud vynesl rozsudek v případu čtyř mužů, obžalovaných z celkem třinácti loupeží v Moravskoslezském kraji. Docházelo k nim od dubna 2012 do března 2013 v Ostravě, na Frýdecko-Místecku a Karvinsku. Lupiči přepadávali banky, ale také pošty, herny a čerpací stanici. Hlavnímu pachateli, Davidu Arbetovi, zpřísnil soud trest na 12 let odnětí svobody, dva další obžalovaní si odpykají pět a devět let, čtvrtý muž byl viny zproštěn. Lupiči se postupem času zdokonalovali. Zpočátku na místo činu dojížděli na kolech a k zastrašení pracovníků využívali například páčidlo. Později si opatřili střelnou zbraň a kvůli rychlé přepravě na místo a z místa činu si půjčovali auta.

Zdroje pro tuto kapitolu: PČR, *cyprus-mail.com, ihned.cz, idnes.cz, europol.europa.eu, ceskatelevize.cz, bakerstreet.wikia.com, novinky.cz, csas.cz, cnb.cz, newmoney.gov, policejnidenik.cz, zive.cz, europeum.org, bvv.cz, banktech.com, sxc.hu, cnn.com, ceskatelevize.cz, denik.cz, lidovky.cz, datarama.aktualne.centrum.cz, policie.cz, brnensky.denik.cz, policejnidenik.cz, zachranny-kruh.cz, btctip.cz, aktualne.cz, computerworld.cz, cnews.cz, bankovnipoplatky.com,*

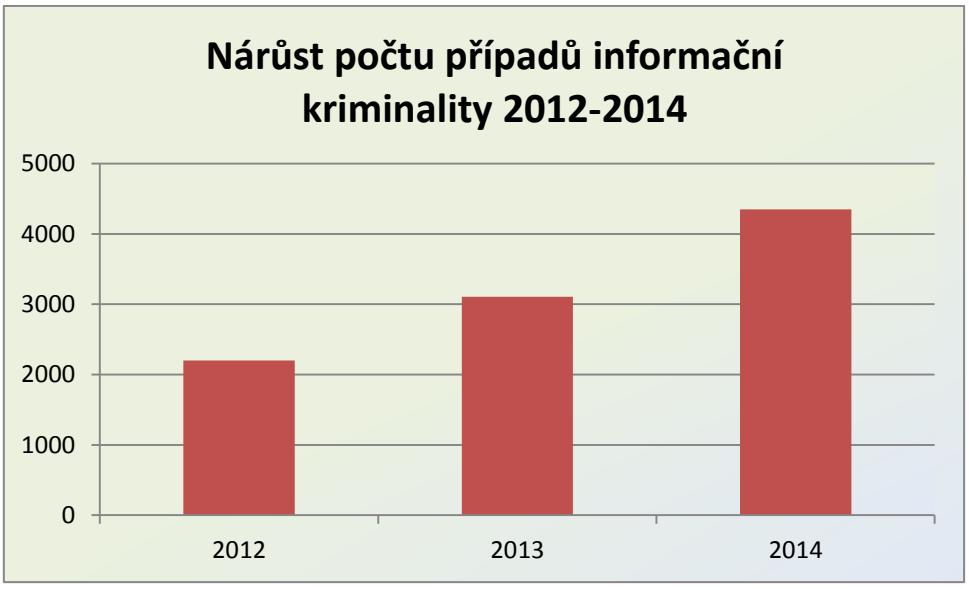
INFORMAČNÍ KRIMINALITA A KYBERNETICKÁ BEZPEČNOST

Policejní statistiky a jejich interpretace

Kybernetická bezpečnost a kriminalita se v celoevropském měřítku dostávají stále více a více do centra pozornosti bezpečnostních složek i států jako takových. Vznikají národní týmy pro řešení kybernetických incidentů, specializované národní i mezinárodní policejní složky, připravuje se nová legislativa i zásadní strategické dokumenty. Česká republika v tomto směru není výjimkou. Tato kapitola shrnuje některé nejdůležitější aktivity veřejné sféry, které v naší zemi v oblasti kybernetické bezpečnosti proběhly, či se v nejbližší době chystají. Nejprve se ale zaměříme na strukturu a rozsah u nás páchané informační kriminality.

Informační kriminalitou rozumíme takovou trestnou činnost, která je **páchána v prostředí informačních technologií**, kdy předmětem útoku je buď samotná oblast informačních technologií, případně je tato trestná činnost prováděna za výrazného využití informačních technologií. Termín informační kriminalita (IK) je tedy označením pro poměrně širokou skupinu trestných činů, které spojuje určitý společný faktor, daný právě formou páchání tohoto typu trestné činnosti. Jedná se nejčastěji o porušování autorských práv, různé podvodné aktivity, krádeže elektronických dat, útoky zaměřené na destabilizaci datových sítí, šíření závadného elektronického obsahu (dětská pornografie, extremistická ideologie), ale také o vydírání, vyhrožování a poměrně nově i o tzv. **stalking** (nebezpečné pronásledování).

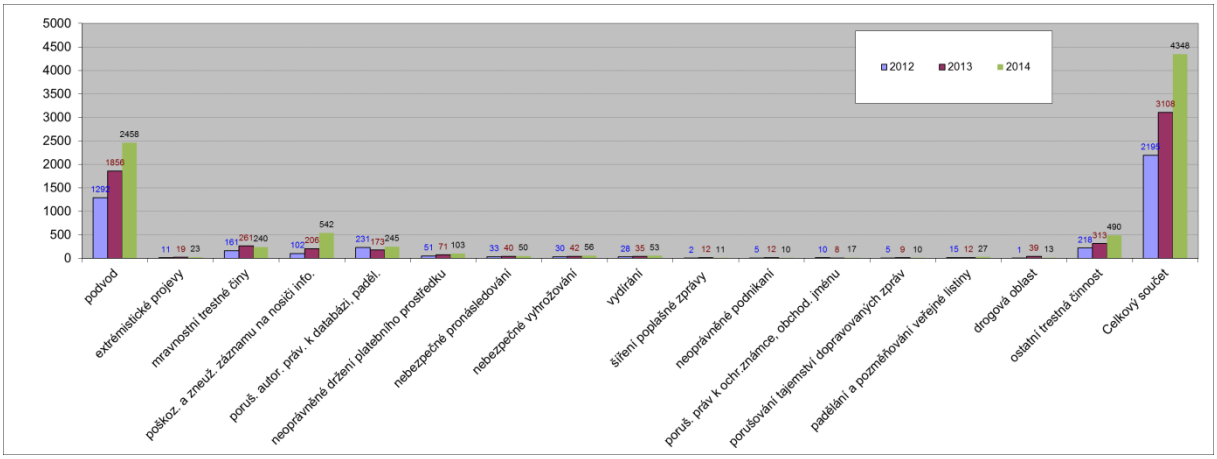
Také v roce 2014 jsme byli svědky pokračujícího rychlého nárůstu informační kriminality v ČR, který jen potvrzuje, že jde o nejdynamičtěji se rozvíjející formu kriminality vůbec. **Zaznamenáno bylo celkem 4348 případů, což oproti roku 2013 představuje nárůst o celých 40%**. Následující graf zachycuje růst počtu případů za posledních několik let, přičemž nelze očekávat, že se tento trend v následujícím roce zpomalí či zastaví.



Počet zaregistrovaných skutků informační kriminality roste celosvětově už mnoho let a vzhledem k tomu, že se stále větší část života a fungování společnosti odehrává právě ve virtuálním prostředí, nelze ani v příštích obdobích očekávat v tomto smyslu změnu. Informační kriminalita tedy představuje nejen jednu z hlavních budoucích výzev pro Policii ČR, ale pro bezpečnostní složky celého světa.

Z přiloženého grafu je dobře patrný meziroční nárůst incidence zaznamenaných případů informační kriminality, ve srovnání s rokem 2013. Porovnání s rokem 2012 vyznívá ještě nepříznivěji – česká policie musela v roce 2014 řešit téměř dvojnásobné množství případů.

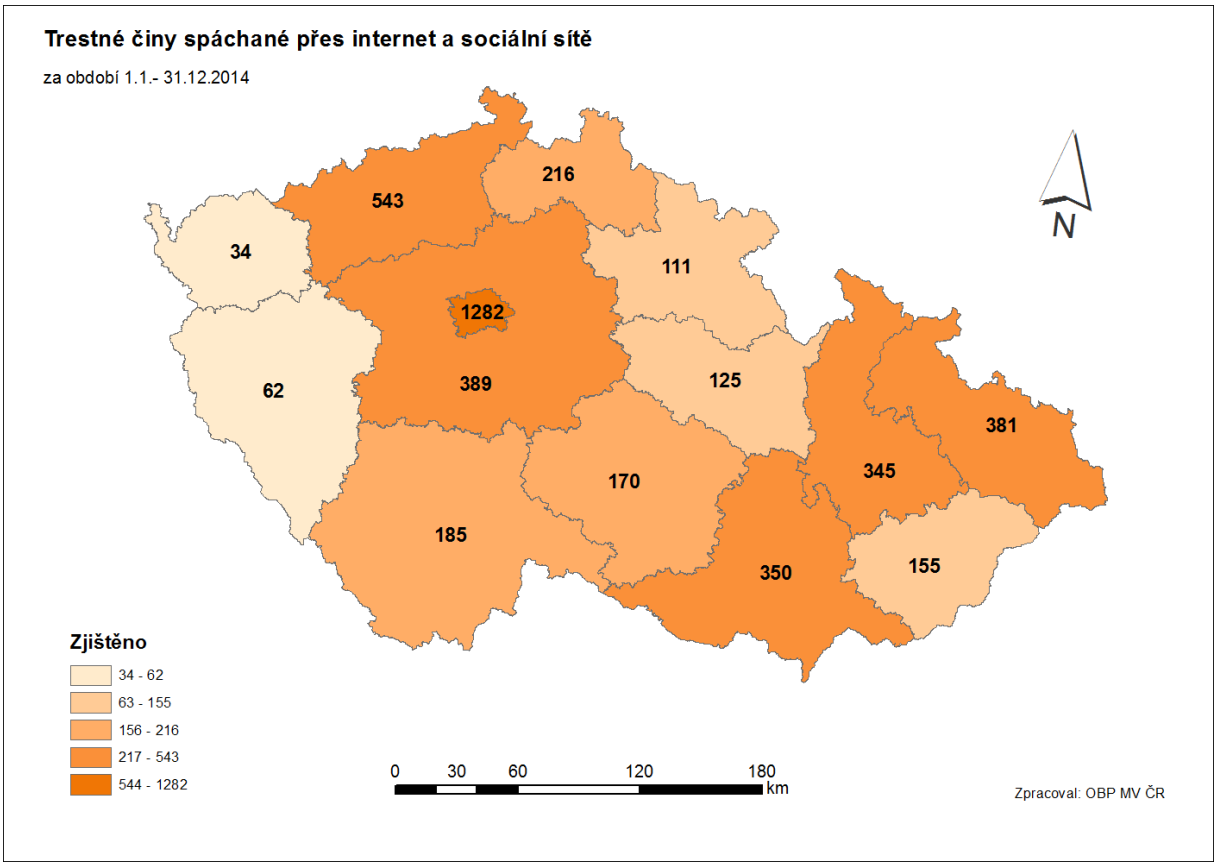
Naopak struktura zaznamenávané trestné činnosti se téměř nemění – stále **výrazně dominují různé formy podvodného jednání**, které i v roce 2014 tvořily více než polovinu všech evidovaných skutků. S velkým odstupem pak následuje poškozování a zneužití záznamu na nosiči informací, případy porušování autorských práv a různé mravnostní trestné činy (např. dětská pornografie). Ve sledovaném období řešila policie také 50 případů tzv. stalkingu (nebezpečné pronásledování). **Nejrychleji ovšem roste segment neoprávněných manipulací s daty, kde byl zaznamenán nárůst trestné činnosti o 163 % oproti roku 2013**.



V oblasti porušování autorských práv v prostředí informačních technologií je stav pouze s mírnými výkyvy v posledním období setrvalý. Potvrdil se plošný přesun výskytu šíření materiálů porušujících autorský zákon do segmentu datových úložišť. Existující výjimkou ve výměnných sítích zůstává tzv. **torrentová služba**, byť její oblíbenost vytrvale klesá. Rovněž tak je patrný i trend využití tzv. **cloudových služeb**, primárně určených ke sdílení elektronických dat mezi jednotlivými technickými zařízeními uživatele či určené pro potřeby komunitních a firemních skupin. Pachatelé využívají při snaze zakrýt své jednání stále častěji kryptovací mechanismy.

Co se týče geografického rozložení informační kriminality, které znázorňuje následující mapa, pak také v roce 2014 přetrvávala **zcela jednoznačná dominance Prahy**. V metropoli je nahlášena **téměř třetina celkového nápadu** této formy trestné činnosti. V této souvislosti je nicméně nutné říci, že informační kriminalita patří mezi vůbec nejproblematičtější z hlediska určení místní příslušnosti. Roli zde hraje např. umístění serverů, poskytovatelů služeb, síťových uzlů atd. Vzhledem k této prostorové neuchopitelnosti informační kriminality je geografické rozložení v rámci ČR spíše orientační

Druhé místo drží kraj Ústecký, kde se odehrává zhruba osmina veškeré zaznamenané informační kriminality v ČR. Naopak překvapivě nízká je incidence v kraji Plzeňském, který patří, společně s krajem Karlovarským, mezi ty nejméně postižené.



Pokračujícím trendem zůstává podle Policie ČR **nárůst aktivity pachatelů na sociálních sítích**. Časté jsou zejména krádeže identit, ať již za účelem kompromitace dané osoby, či kvůli využití její identity jako legendy pro páchání podvodných jednání. Sociální sítě jsou zneužívány stále více také k projevům nebezpečného pronásledování (stalking) a tzv. **kyberšikany**.

Doslova exponenciální růst zažívají (stejně jako v minulých letech) útoky formou tzv. **phishingu**. Cílem je zejména získat podvodný přístup na bankovní účty, z nichž jsou pak neoprávněně odčerpávány finanční prostředky., Časté je zneužití předem vytvořeného prostředí ve formě tzv. botnetů, tedy útok vytvořených cílových stanic, určených přes rozličné architektury sítí k páchání dalších kriminálních aktivit.

Podobná profesionalizace systému je pak patrná i ve variantě aktivních odkazů, odkud oběť kompromituje svůj vlastní systém, jehož činnost již v další fázi ovládá pachatel. V letošním roce se jednalo o několik masivních vln zmíněných **phishingových útoků na zákazníky bankovních institucí**, které probíhali souběžně na PC i na mobilních zařízeních, přes něž jsou prováděny nejčastěji autorizace přístupů do bankovních účtů. Ze strany pachatelů je naprosto zřejmá zvyšující se profesionalizace, spolu s rostoucí masivností takových typů útoků, **kterých byl v uplynulém roce největší počet jak co do počtu, tak i co do masivnosti v celé historii ČR**.

V listopadu 2014 se velmi rozšířily **podvodné e-maily, které se vydávaly za zprávy od České pošty**. Ty mohou do počítače stáhnout škodlivé programy a zneužít citlivá data. Podvodné e-maily jsou psány ve formě 'Informace o Vaší zásilce', kde najde klient údaje o nedodání a odkaz pro stažení informací o zásilce, který již vede na podvodnou webovou

stránku. Zprávy byly rozesílány z adres support@cs-post.net, tracktrace@cs-post.net, cpost@cs-post.net, post@cs-post.net, zasilka@cs-post.net a pravděpodobně i některých dalších. Česká pošta kvůli nim podala trestní oznámení na neznámého pachatele.

Jiné emaily, před kterými Policie ČR varovala v červenci, **vyzývají k úhradě dlužných částek neexistujících exekucí**. K tomu je vhodné uvést vyjádření mluvčí Exekutorské komory ČR: „*Exekutorské úřady neposílají exekuční příkazy prostřednictvím emailových zpráv, pokud tedy o to účastník řízení sám nepožádá. V případě, že účastník řízení si vyžádá poslání exekučního příkazu e-mailem, tento příkaz se zasílá ve formátu „pdf" a je podepsán elektronickým podpisem příslušného exekutora*".

Dle Exekutorské komory ČR by měl písemný exekuční příkaz mimo jiné obsahovat:

- označení exekučního soudu,
- označení soudního exekutora, který na základě pověření soudu vede exekuční řízení (seznam exekutorských úřadů naleznete na stránkách Exekutorské komory ČR),
- exekuční titul a orgán, který jej vydal, nebo osobu, která jej vyhotovila,
- označení účastníků včetně rodného čísla povinného,
- způsob provedení exekuce,
- označení osob, jimž se doručuje exekuční příkaz,
- výrok, poučení o odvolání, den a místo vydání exekučního příkazu a podpis soudního exekutora.

V případě, že se uživatelé setkali s tímto e-mailem, doporučujeme provést důslednou antivirovou kontrolu celého zařízení. Pokud došlo k otevření přílohy popsaného emailu, pak je možné konstatovat, že počítačový systém je s největší pravděpodobností kompromitován malwarem a v takovém případě je nutné jeho odborné odstranění.

Na našem území není častý výskyt organizátorů takovéhoto jednání, nicméně stálý je výskyt tzv. **bílých koní**, jinak též „e-mules", kteří mají za úkol převzít na svůj účet neoprávněně odčerpané prostředky z účtu poškozeného a ty jiným platebním kanálem poslat dále tak, jak jsou instruováni. Často pachatelé své bílé koně nějakou dobu skutečně „zaměstnávají" tj. nechávají je posílat peníze ze svého účtu na cizí a dávají jim za to směšné provize (často v řádu stokorun – lidé jsou ovšem spokojení, že dostávají plat téměř bez práce). Případně je využívají k dalším činnostem ve chvíli, kdy je nutné nějakým způsobem jednat s úřady, s aukčním portálem (falešné zboží obvykle inzeruje „bílý kůň") atd. Policie sice bílého koně mnohdy poměrně snadno odhalí, jedná se ale často o lidi, kteří jsou skutečně upřímně přesvědčení, že pracovali jako „finanční manažeři" pro významnou zahraniční firmu, jejíž zástupce nikdy v životě neviděli. Mnohdy jsou překvapeni, že sloužili jen pro krytí trestné činnosti. O svých „zaměstnavatelích" mají přitom minimum informací, které obvykle nelze pro další vyšetřování použít. Ačkoliv nemalá část bílých koní vůbec netuší, že se podílí na ilegálních aktivitách, hrozí jim stíhání za podíl na legalizaci výnosů z trestné činnosti.

Bílí koně jsou zneužíváni také k vytváření **falešných internetových obchodů**. Nabízejí obvykle elektroniku či jiné žádané (a přitom snadno transportovatelné) zboží za velmi výhodné ceny. Falešný e-shop se dá nejlépe odhalit tak, že se pokusíme si na internetu najít nějaké recenze na jeho činnost (i ty se ale podvodníci snaží často falšovat), jeho historii, a zkontroluji, zdali zveřejňuje všechny údaje, které o svém podnikání zveřejňovat má. Dobrým indikátorem je také to, že falešné e-shopy (na rozdíl od těch solidních) prakticky nikdy nenabízejí dodávku zboží na dobírku. Obvykle jsou zakládány na omezenou dobu a po pár týdnech beze stopy zmizí, aby se zase pod novou grafikou a novým názvem objevily jinde na internetu. Fiktivní internetové obchody také někdy slouží ke krytí zdrojů a původu financí pocházejících z trestné činnosti.

V roce 2014 poklesl naštěstí výskyt tzv. **ransomware**, tedy vyděračských virů, které požadují „vykupné“ za to, že zabrání ztrátě veškerých dat. V České republice byla nejrozšířenější variantou viru ta, která zobrazí fiktivní upozornění Policie ČR, že byl na počítači zjištěn ilegální obsah a použití přístroje bude proto blokováno do zaplacení příslušné pokuty. Tento virus byl nejrozšířenější v roce 2013, ale v roce 2014 bylo stále zaznamenáno několik případů. Oproti pokročilejšímu ransomware Cryptolocker, který data v počítači neprolomitelně zašifroval, je česká varianta viru odstranitelná odborným technickým zásahem.

Nezanedbatelné jsou podvodné aktivity v rámci **aukčních portálů**, kde se mimo podvrhy objevují masivně i věci pocházejících z trestné činnosti a věci, jejichž volná distribuce není povolena. Stále se rozšiřující projev u podvodných jednání je nárůst vyvádění finančních prostředků do **virtuálních měn**. Tyto měny jsou rovněž často využívány i k platbám za obchody s nedovoleným zbožím, včetně drog a zbraní, nejčastěji prostřednictvím sítě TOR. Fenoménu virtuálních měn byla věnována obsáhlejší analýza v předchozí situační zprávě.

S rostoucí oblibou anonymizačních služeb dochází i k nárůstu počtu případů **vydírání**, který byl v roce 2014 meziročně více jak 50%. To je doprovázeno i sílící intenzitou hrozeb. Naopak v loňském roce nebyly zaznamenány tak masivní DDoS útoky na základní veřejné služby, k jakým došlo v říjnu 2013.

Pokud se týká rizik vyplývajících ze znemožnění zjištění identit pachatelů ze strany Policie ČR, je nutné poukázat na nebezpečí šíření anonymního připojení do sítě internet prostřednictvím volně přístupných Wi-Fi bodů a anonymního připojení z předplacených karet mobilních operátorů. Na druhou stranu také dochází ke sběru citlivých dat uživatelů z **podvrhnutých Wi-Fi hot spotů**.

Z nastíněných trendů lze dovodit, že **profesionalizace pachatelů informační kriminality** bude vykazovat stále větší míru propracovanosti s jasnější dělbou jednotlivých rolí. Větší by mohlo být i zapojení tzv. botnetových sítí, které mají za úkol anonymizovat aktivitu původce nelegálního jednání a současně **zvyšovat masivnost či technologickou koordinaci útoku**. V delším výhledu pak je zcela zjevné, že s ohledem na optimalizaci nákladů a dostupnost přístupu, výměnu a archivaci veškeré komunikace, bude většina nepřímé komunikace digitalizována. Bude neustále růst objem a rozsah veškerých takto zaznamenávaných lidských aktivit. To se týká nejen běžného druhu obsahu, ale stejně tak i citlivých, osobních či jinak chráněných dat. V tomto ohledu bude exponenciálně růst míra důležitosti ochrany a nutnosti adekvátního opatření při narušování této ochrany, která ve většině případů bude mít kriminální charakter.

Další často řešenou problematikou z pohledu Policie ČR na internetu je **ochrana dětí**. Dětská pornografie se obvykle šíří v rámci uzavřených komunit, které tyto materiály vzájemně sdílí. Přesto se policii daří pravidelně tyto struktury narušovat. Dané materiály jsou často šířeny tajně přes elektronickou poštu, úložný prostor, či přes přímou výměnu instant messengerů. Stále četnější jsou také snahy získávat materiály intimního až pornografického charakteru přímo od dětí prostřednictvím sociálních sítí.

Jedná se přitom často o velmi malé děti, což je odrazem faktu, že rodiče mnohdy nemají nejmenší přehled o tom, co jejich ratolesti na internetu dělají. Ačkoliv to firemní pravidla zakazují, facebookové profily třináctiletých dětí nejsou vůbec výjimkou (Facebook je maže jen po upozornění). Tyto děti se tak mohou stát snadnou obětí sexuálních útoků (pachatelé často vystupují také pod dětskou identitou), případně kybernetické šikany.

Kromě dětí jsou další velmi ohroženou skupinou na internetu senioři. Právě do kybernetického prostředí totiž přesouvají část svých aktivit agresivní prodejci, kteří starším lidem nabízejí nevýhodné smlouvy a nekvalitní zboží. Kontaktují seniory pomocí inzerátů, nevyžádaných e-mailů a sociálních sítí. Na tyto problémy upozorňuje také Národní centrum bezpečnějšího internetu. Elektronickou poštu od podvodníka podle něj obdržely letos tři čtvrtiny Čechů. V případě seniorů se také velmi rozmáhá citové vydírání, např. prostřednictvím seznamek a sociálních sítí. Podvodníci pod smyšlenou identitou navážou s obětí důvěrný vztah a pak se snaží například vylákat peníze na léčbu vážné nemoci. Podle Soudkové se internetové nabídky týkají předraženého zboží a smlouvy se uzavírají často telefonicky pod nátlakem. Podle neziskové organizace Život 90, která poskytuje služby a pomoc seniorům, jsou terčem internetových podvodů ročně tisíce starších lidí a jejich počet prý strmě roste.

Pro informační kriminalitu je bohužel typická mimořádně **vysoká míra latence**, takže o drtivém množství útoků se policie vůbec nedozví. Pokud sečteme odhadované počty automatizovaných i cílených útoků, úspěšných i neúspěšných, dostáváme se k hodnotám kolem 200 tisíc incidentů denně jen v České republice. Ve světě přitom nejde o nikterak mimořádná čísla (značnou část z nich mají ovšem na svědomí automatizované botnety).

Policie se snaží usnadnit veřejnosti hlášení incidentů informační kriminality a zřídila za tímto účelem **internetovou Hotline**, což je fakticky on-line formulář, který je veřejnosti zpřístupněn na internetových stránkách www.policie.cz. Prostřednictvím tohoto formuláře mohou občané jednoduše hlásit závadný obsah a závadové aktivity v síti internet. Odborné pracoviště Hotline PČR je součástí odboru informační kriminality úřadu služby kriminální policie a vyšetřování Policejního prezidia České republiky a jeho pracovníci evidovali za rok 2014 celkem 6590 podnětů směřovaných právě do oblasti kybernetického prostředí, což je oproti roku 2013 nárůst o celých 72%.

Aktivity ČR v oblasti kybernetické bezpečnosti

V rámci kybernetické bezpečnosti se stát snaží zajistit odolnost informačních systémů a sítí před různými typy hrozeb. Fungování současné společnosti je stále více závislé na informačních technologiích a informačních systémech – při jejich výpadku, napadení či zneužití hrozí často obrovské škody a mohou být narušeny některé základní funkce, které má stát pro své občany zabezpečovat (např. zajišťování bezpečnosti, výplata důchodů a sociálních dávek atd.).

národní centrum kybernetické bezpečnosti

Gestorem a národní autoritou pro oblast kybernetické bezpečnosti je, na základě usnesení vlády ČR č. 781 ze dne 19. října 2011, **Národní bezpečnostní úřad (NBÚ)**. Na základě téhož usnesení vzniklo v Brně **Národní centrum kybernetické bezpečnosti (NCKB)**, jehož úlohou je koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům i při návrhu a přijímání opatření při řešení útoků probíhajících. **Ke slavnostnímu otevření sídla tohoto centra došlo dne 13. května 2014**, řadu činností ovšem vykonávalo NCKB už od září 2012.

Jeho klíčovou součástí je tzv. **vládní CERT**, který hraje důležitou roli při ochraně kritické informační infrastruktury a významných informačních systémů podle nového zákona o kybernetické bezpečnosti (181/2014 Sb.), o němž jsme podrobněji informovali v předchozí situační zprávě. Více informací o činnosti těchto institucí lze nalézt na následujícím odkazu:

http://www.govcert.cz

Za rok 2014 bylo pracovníkům NCKB/GovCERT.CZ **oznámeno 85 incidentů**, přičemž 82 z nich se podařilo v tomtéž roce vyřešit. Nejčastějšími typy řešených incidentů byly škodlivé kódy a útoky na bázi sociálního hackingu (např. phishing). 43 útoků bylo zacíleno na veřejný sektor, 35 na soukromý sektor, 2 na kritickou infrastrukturu a v 5 případech byla také poskytnuta podpora při řešení incidentů fyzickým osobám.

Dobrý přehled o aktivitách České republiky v této oblasti může poskytnout také vládou schválená **Zpráva o stavu kybernetické bezpečnosti v roce 2014**. Ta shrnuje informace o plnění hlavních cílů v nejdůležitějších oblastech zajišťování kybernetické bezpečnosti. V uplynulém roce se podařilo dosáhnout velkého pokroku v oblasti legislativní, když se, kromě samotného zákona č. 181/2014 Sb. o kybernetické bezpečnosti, podařilo připravit či upravit i všechny související právní předpisy. Jedná se zejména o:

- **vyhlášku č. 316/2014 Sb.**, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti;
- **vyhlášku č. 317/2014 Sb**., o významných informačních systémech a jejich určujících kritériích;
- novelu **nařízení vlády č. 432/2010 Sb.** ze dne 22. prosince 2010, o kritériích pro určení prvku kritické infrastruktury

Poslední jmenované nařízení připravil NBÚ ve spolupráci s Ministerstvem vnitra, neboť je tento předpis v gesci MV-Generálního ředitelství Hasičského záchranného sboru ČR. V době přípravy této situační zprávy na počátku roku 2015 byly již všechny tyto předpisy schváleny a vstoupily v platnost.

Národní bezpečnostní úřad zároveň připravil novou **Národní strategii kybernetické bezpečnosti na období let 2015 až 2020** a na ni navazující **Akční plán**. Jedná o klíčové dokumenty, které nastavují směřování této problematiky v příštích letech. Jelikož jejich schválení proběhne v 1. pololetí roku 2015, budeme jim věnovat více pozornosti v příští situační zprávě.

Na mezinárodní úrovni došlo zejména k zapojení České republiky do **NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) v Tallinnu**, jehož cílem je zvyšovat obranné schopnosti a zlepšovat spolupráci a sdílení informací mezi účastnickými státy a NATO, popřípadě mezi účastnickými státy navzájem a také partnery v oblasti kybernetické obrany. Rovněž se podařilo zrealizovat zařazení GovCERT.CZ na seznam Trusted Introducer organizace Trans-European Research and Education Networking Association TI.

Na evropské úrovni probíhala také spolupráce s **Evropskou agenturou pro bezpečnost sítí a informací (ENISA)**, kde má Česká republika v současnosti své zastoupení formou účasti na formálních a neformálních jednáních. Dva zástupci NBÚ jsou členy vedení ENISA , které je zodpovědné za schvalování programu a rozpočtu agentury. Na podzim roku 2014 byl osloven pracovník NCKB, aby se stal členem užší pracovní skupiny ENISA vytvořené na podporu tvorby a implementace národních strategií kybernetické bezpečnosti.

V roce 2014 se Národní centrum kybernetické bezpečnosti zúčastnilo celkem šesti národních a mezinárodních cvičení. V průběhu roku 2014 se NCKB účastnilo několika mezinárodních cvičení. Jednalo se zejména o cvičení **Cyber Coalition 2014**, které mělo za cíl otestovat připravenost států NATO na kybernetické útoky, především pak na schopnost efektivně rozhodovat při zvládání kybernetických krizí, schopnost států vyměňovat relevantní informace pro jejich řešení, či potřebné technické a právní kapacity. Mimo 26 členských států NATO se cvičení zúčastnilo pět partnerských zemí a zástupci kybernetické obrany Evropské unie.

Cvičení Cyber Coalition 2014 (CC14) začalo 17. listopadu a trvalo do 21. listopadu 2014, řízeno bylo opět z Estonského Tartu. Jako obvykle mělo prověřit rozhodování a koordinaci mezi orgány NATO a národními kybernetickými obrannými kapacitami, včetně partnerských zemí. Novinkou proti předchozím ročníkům bylo pozvání zástupců z akademické sféry a průmyslu všech zúčastněných států. NATO se tímto snaží více zapojit výzkum a průmysl do kybernetické obrany.

Z České republiky se CC14 zúčastnilo zatím nejvíce subjektů v jeho historii. Jak již bylo uvedeno, koordinaci české strany měl na starosti NBÚ společně s Ministerstvem obrany (MO). Do cvičení se jim podařilo proti předchozím ročníkům zapojit více aktivních cvičících, kterými byly, kromě vlastních týmů Vládní CERT a CIRC-MO, odborníci z Policie České republiky, zpravodajských služeb, bezpečnostních týmů CSIRT.CZ, CZ.NIC, CSIRT MU a další. V neposlední řadě se zapojili i odborníci na právo z NBÚ, MO, Ministerstva zahraničních věcí a Masarykovy univerzity, kteří řešili právní problémy společně s právníky z CCDCoE v Estonsku.

ČR se také aktivně zúčastnila cvičení **Locked Shields 2014** pořádané NATO CCDCOE, které bylo zaměřeno zejména na technickou a zčásti i právní část řešení kybernetických útoků. Při tomto cvičení vytvořila Česká republika společný tým s Lotyšskem, přičemž výsledkově se v obou částech cvičení umístila na předních příčkách. Česká republika se také podílí na tvorbě scénářů ke cvičení Crisis Management Exercise (CMX) v rámci NATO, jehož provedení bylo odloženo na rok 2015.

Zároveň se v loňském roce uskutečnilo první velké **národní cvičení CYBER CZECH 2014**. To proběhlo dne 6. října 2014 v prostorách Národního bezpečnostního úřadu. Cvičení proběhlo formou table-topu a jeho hlavním cílem bylo procvičit procesy nezbytné ke zvládání a řešení DDoS a phishingových útoků. Byla otestována funkčnost stávajících mechanismů a prověřena výměna informací včetně ověření spolupráce mezi veřejným a soukromých sektorem. Procvičovány byly konkrétní scénáře obou typů útoků, jejichž součástí bylo krátké uvedení do situace následované zadáním úkolů a vypracováním jejich řešení. Po vypršení časového limitu vždy proběhla diskuse s odborníky z dotčených oblastí, na jejímž závěru byla vybrána optimální řešení zadaných úkolů, mimo jiné s ohledem na nový zákon o kybernetické bezpečnosti. Cyber Czech 2014 se aktivně zúčastnili zástupci bezpečnostních odborů Úřadu vlády, ministerstev vnitra, dopravy, financí, obrany, průmyslu a obchodu, zahraničních věcí, práce a sociálních věcí, spravedlnosti, životního prostředí a školství, mládeže a tělovýchovy. Dále lidé z bezpečnostních odborů z Úřadu pro ochranu osobních údajů, Českého telekomunikačního úřadu, České národní banky a Národního bezpečnostního úřadu.

Jejich konání a návrhy postupů hodnotili a doplňovali odborníci z různých oblastí, konkrétně zástupce národního bezpečnostního týmu CSIRT.CZ, zástupce globálního poskytovatele internetové sítě a odborníci z NCKB. Dále zástupci ze státního zastupitelství, právní teoretik se specializací IT, zástupci Policie ČR se zaměřím na informační kriminalitu a zástupci zpravodajských služeb.

Význam kybernetického cvičení umocnil svou návštěvou policejní prezident plk. Tomáš Tuhý, který sledoval plnění jednoho ze zadaných úkolů přímo na půdě NBÚ. Z jeho hodnocení akce vyplynulo, že oblast kybernetické bezpečnosti bere z titulu své funkce velmi zodpovědně a první české cvičení ohodnotil pozitivními slovy.

Z dalších proběhlých cvičení roku 2014 lze ještě telegraficky zmínit např. Cyber Europe, EU-Multi Layer, CECSP atd. V roce 2014 byla také rozvíjena bilaterální spolupráce v oblasti kybernetické bezpečnosti s partnerskými státy. Za významné lze považovat Společné prohlášení o spolupráci v oblasti kybernetické bezpečnosti, které dne 25. listopadu 2014 podepsali v Jeruzalémě zástupci Izraele a České republiky.

Nové hrozby v oblasti kybernetické bezpečnosti

Nová hrozba: Shellshock

Během září 2014 byla identifikována nová softwarová chyba, označovaná jako Shellshock (původně též „Bashdoor“). Využívá zranitelnosti v rozšířeném unixovém shellu Bash, tedy v rozhraní, které pro svou činnost využívá řada „na pozadí“ (tj. bez přímé interakce s uživatelem) běžících programů. Tyto programy, kterým se říká také „démoni“ se obvykle spouští při startu systému a samostatně obsluhují např. počítačové sítě, tiskové fronty apod.). Velké množství démonů je také součástí webových serverů.

Skrze zranitelnost Shellshock může útočník na dálku ovládnout řadu takových programů a přimět je vykonávat libovolné příkazy. Závažnost chyby je dána rozšířeností shellu Bash, takže mohla být teoreticky zneužita k napadení milionů serverů a jiných systémů. Potenciální rozsah problému se tak přibližoval i tzv. chybě krvácejícího srdce (Heartbleed Bug), o které jsme informovali v minulé situační zprávě.

Je přitom zajímavé, že bezpečnostní mezera Shellshock byla součástí zdrojových kódů už od roku 1992, po celých 22 let ji tedy někdo mohl teoreticky zneužívat. V současné době by již měly být bezpečnostní mezery záplatovány, vzhledem k rozsahu potenciální hrozby je ale vhodné věnovat i nadále zabezpečení unixových shellů pozornost.

Další hrozby ve sledovaném období

Ve sledovaném období došlo k velkému rozšíření malwaru **Cryptowall**, který je další verzí pokročilého ransomware Cryptolocker, o kterém jsme již informovali v předchozích situačních zprávách. Počítač se nakazí obvykle skrze zavirovaný email a následně jsou data v něm zašifrována. Virus požaduje výkupné v bitcoinech. Prozatímního vrcholu svého rozšíření dosáhl v říjnu 2014, a to zejména ve Spojených státech a v Japonsku. Několik případů bylo ale podle společnosti Symantec zaznamenáno i v ČR.

Na konci května 2014 došlo k mezinárodnímu zásahu proti botnetu **Gameover Zeus**, na kterém byl provozován také velmi úspěšný ransomware Cryptolocker („otec“ Cryptowallu). Ten za pár měsíců své existence nakazil zhruba čtvrt milionu počítačů a podle odhadů na výkupném inkasoval přes 27 milionů dolarů. Na akci se podílela řada vyšetřovatelů, od Kanady, přes Francii a Německo, až po Japonsko a Nový Zéland. Rozhodující roli v koordinaci všech složek hrála americká FBI a evropské centrum EC3. Vůdcem skupiny, která Zeus provozovala, byl 30letý muž z ruské Anapy.

V říjnu 2014 dále došlo k pravděpodobnému **úniku 7 milionů hesel z populární on-line úschovny Dropbox**. Hackeři seznam zveřejnili na internetu, Dropbox ještě před tímto krokem tato hesla zneplatnil (řada z nich měla platnost již vypršelou). Někteří uživatelé tak mohli mít problém s přístupem ke svým souborům. V rámci úniku údajně nedošlo přímo k infiltraci Dropboxu, ale služby třetí strany, jejíž uživatelské účty jsou na Dropbox napojeny. Jako preventivní opatření se doporučuje zavést si na on-line úložištích dvoufaktorovou autentizaci a také nepoužívat stejné heslo do více služeb (např. do úschovny i do emailu).

Fenomén: rizika Smart Homes

V nedávné době proběhla řadou médií zpráva o tom, že televize od jihokorejské společnosti Samsung odposlouchávají své diváky a následně tyto citlivé informace předávají jiným firmám. Televizor Smart TV má totiž nainstalovanou funkci pro ovládání hlasem - není tak třeba používat dálkový ovladač a na přístroji je možné např. nastavit hlasitost či přepnout program pouze s pomocí slovního příkazu.

V manuálu výrobku lze nalézt upozornění, že v rámci snahy o vylepšování služby jsou hlasové příkazy, zachycené mikrofony přístroje, odesílány k vyhodnocení třetí straně. Zároveň je manuálu varování, že **mikrofony mohou (logicky) kromě samotných příkazů zachytit také veškeré další zvuky a hlasy v místnosti, včetně např. citlivých nebo osobních rozhovorů**. Výrobce upozorňuje, že také tyto informace mohou být nahrány a poslány třetí straně.

Jelikož celá záležitost nápadně připomíná některé pasáže z Orwellova slavného románu „1984“, vyvolala zpráva značnou vlnu znepokojení. Ve zmíněné knize jsou televizní přístroje zneužity totalitním režimem ke šmírování lidského soukromí a slouží jako jeden z nástrojů absolutní kontroly státu nad nesvobodnou společností. Skandál s „chytrou“ televizí od společnosti Samsung tak vyvolává dojem, že Orwellova (ve své době ještě utopistická) vize nyní dochází svého naplnění.

Pro úplnost je potřeba uvést, že srovnávání současné aféry Samsungu s orwellovským zotročováním společnosti je (jakkoliv se nabízí) poněkud přehnané a nepříliš spravedlivé – realita v pozadí této události je mnohem méně děsivá a daleko prozaičtější. Hlasové ovládání představuje logický další krok ve vývoji (nejen) televizních přístrojů a Samsung neudělal nic jiného, než že se s pomocí získaných dat pokoušel tuto funkci (která je stále ještě ve svých počátcích a má řadu nedostatků) vylepšovat - k tomu je pochopitelně potřeba velké množství srovnávacích záznamů, které se nejlépe získávají právě z již prodaných přístrojů. **Nic nenasvědčuje tomu, že by firma byla vedena jinými motivy a získaná data skutečně zneužívala** (např. k marketingu).

Smart TV totiž nenahrává dění v místnosti neustále – **uživatel přístroje musí hlasové ovládání povolit** (a může jej kdykoliv vypnout) a záznam je pořizován pouze ve chvíli, kdy stiskne a drží příslušné tlačítko. Je poměrně logické, že v takovou chvíli mikrofony zaznamenají kromě hlasových příkazů také veškeré další zvuky v místnosti. Samsung tyto skutečnosti zcela otevřeně v manuálu uvádí, a pokud uživatel při používání televizoru na toto omezení myslí (a neříká nic osobního v době, kdy přístroji zadává hlasové příkazy), k žádnému „odposlechu“ citlivých údajů by nemělo dojít. Samsung pak dle svého vyjádření poskytuje získané údaje pouze firmě Nuance Communications, která pro něj systém rozpoznávání hlasu vyvíjí. Online přenos dat mezi televizorem a firmou je údajně šifrovaný.

Samsung navíc **není zdaleka jediný, který využívá online sběru dat z vlastních prodaných přístrojů k vylepšování svých služeb**. Podobné varování měly ve svých manuálech uvedeny i některé výrobky společnosti LG, automobilka GM zase prostřednictvím služby OnStar shromažďuje data o používání svých vozů (např. rychlost, použití bezpečnostních pásů, ale také poloha). Ve skutečnosti obdobných praktik využívá celá řada firem, teprve aféra Samsungu ale vedla k zamyšlení nad jejich potenciálními riziky. A to je jen dobře.

Celá záležitost je totiž součástí širšího fenoménu – tzv. internetu věcí (IoT). Právě jeho bezpečnostním rozměrům a uplatnění v běžných domácnostech (Smart Homes) je věnována tato analýza.

Jak „chytré“ mohou být naše domovy

Po raketovém nástupu tzv. chytrých telefonů (smart phones), o jejichž bezpečnostních rizicích jsme již pojednávali v jedné z předchozích situačních zpráv, jsou stále běžnější součástí naší každodennosti prvky tzv. **chytrých domácností (smart homes)**. Právě ty představují v oblasti IT (společně s mobilními zařízeními) **jednu z největších bezpečnostních výzev současnosti a blízké budoucnosti**.

Uvědomuje si to i Evropská agentura pro síťovou a informační bezpečnost (ENISA), která v prosinci 2014 vydala zajímavou analýzu **Threat Landscape and Good Practice Guide for Smart Home and Converged Media**. Tato analýza obsahuje soupis hlavních hrozeb, které vyplývají z používání pokročilých informačních technologií v domácnostech a stojí za to se na některé z jejích poznatků zaměřit blíže.

O tom, že globální síť internet zásadním způsobem proměňuje fungování moderní společnosti, není potřeba dlouze debatovat. Internetové připojení bylo ovšem velmi dlouho téměř výhradně výsadou stolních počítačů a není to tak dávno, kdy jsme si velmi rychle začali zvykat na to, že internet pronikl také do mobilních telefonů, tabletů, televizorů či automobilů. Odsud je pochopitelně jen krůček k tomu, aby se na internet dokázala připojit také vaše lednička, pračka, vysavač, anebo rychlovarná konvice. Právě toto **pronikání globální sítě do oblastí života, které byly až dosud přísně „offline“**, je podstatou fenoménu, který bývá označován jako **„internet věcí“ (Internet of Things – IoT)**.

Běžné přístroje s pokročilými funkcemi (případně s vlastním operačním systémem) a připojením na internet bývají obvykle, po vzoru „smart phonů“, označovány rovněž příponou „smart“. Pokud máte **vlastní domácnost vybavenou větším množstvím takových „chytrých“ zařízení, které jsou navíc vzájemně kompatibilní a ovladatelné z jedné platformy**, stává se z Vašeho domova „**smart home**“.

A k čemu je vlastně takové ledničce dobré internetové připojení a vlastní operační systém? Chytrá lednice dokáže například rozpoznat vlastní obsah, vyhledat si z databáze vhodné recepty a nabídnout vám, jaké menu si můžete vytvořit ze surovin, které se v ní aktuálně nacházejí. Dokáže poznat, že Vám dochází nějaká důležitá potravina (např. mléko) a včas objedná ze supermarketu nové balení, přičemž rovnou zaplatí Vaší přednastavenou kreditní kartou atd. Toto všechno není žádná sci-fi, **obdobné přístroje již v současné době existují**. **Jejich masovější rozšíření je pak nejspíše otázkou několika málo let, neboť jsou tyto technologie každým rokem cenově dostupnější**.

Je poměrně logické, že internet věcí, tak jako každý technologický pokrok, přináší obrovské možnosti i nemalá rizika. **Chytré domovy mohou výrazně usnadnit vykonávání běžných denních činností**. Jejich možnosti mohou znamenat výrazné zlepšení kvality života zvláště pro seniory (což je vzhledem ke stárnoucí populaci důležité), ocení je také lidé s různým typem handicapu. Výhody mají ale teoreticky přinášet všem – jedním z hlavních atributů chytrých zařízení je jejich schopnost „učení“, tj. **rozpoznání preferencí a návyků jejich uživatelů**. Díky tomu bude každý takový přístroj přesně odpovídat vašim potřebám a aktuálním požadavkům, které brzy už nebudete muset ani vyslovit, protože je odhadne na základě Vašich obvyklých preferencí. Příkladem je chytré osvětlení, které rozezná jednotlivé obyvatele domu a při příchodu do místnosti automaticky ztlumí světla či změní jejich barvu podle toho, jaký světelný komfort daný člověk upřednostňuje. Případně po odchodu otce z kuchyně a příchodu syna automaticky přeladí rádio na synovu oblíbenou stanici.

Další výhodou smart homes je to, že se veškeré jejich komponenty dají ovládat přes internet (tedy např. prostřednictvím chytrého telefonu z postele, ale také například z dovolené). Váš **telefon či tablet se tedy může stát jakýmsi dálkovým ovladačem pro kontrolu celého domu a to z kteréhokoliv místa na světě**. Pokud si nejste jisti, že jste nezapomněli před odletem do Japonska vypnout troubu nebo zhasnout světla, můžete si to na tabletu na dálku zkontrolovat třeba po příletu na letiště v Tokiu a případně obě zařízení přes internet vypnout. Můžete na dálku ovládat topení, vyluxovat dům, anebo nakrmit svého psa. To vše je jistě skvělé, je ale dobré si uvědomit, že **tak rozsáhlé možnosti dálkového přístupu nejsou bez rizika** – zvlášť když se k ovládání vašeho domu může dostat bez vašeho vědomí někdo jiný.

V předminulé situační zprávě jsme upozorňovali na rizika spojená s mobilními zařízeními a upozorňovali jsme na nejčastější chybu, které se dopouštějí majitelé smart phonů, když ke svému přístroji stále přistupují jako k „telefonu“, i když se ve skutečnosti jedná spíš o malý počítač. A jako každý počítač je i smart phone přístupný kybernetickým útokům, možné nákaze počítačovým virem atd. V souvislosti s fenoménem smart homes je tedy nutné toto varování rozšířit – **potenciálnímu kybernetickému útoku může být vystaveno jakékoliv zařízení, které má přístup na internet**, což může nově znamenat také například vysavač, pračku, anebo plynový kotel.

V předchozí situační zprávě jsme také prezentovali statistiky, které dokládají, že zatímco většina lidí ví, že je vhodné mít na svém PC nainstalovaný např. antivirový program, již daleko méně lidí si totéž uvědomuje v případě svého chytrého telefonu a ještě méně lidí si nejspíš něco podobného připustí u „chytré“ rychlovarné konvice. Bohužel si to často neuvědomují ani výrobci „chytrých“ rychlovarných konvic, které sice zajistí, že právě v čas, ve kterém obvykle vstáváte do práce, budete mít již připravenou horkou vodu na kávu, ale jejich zabezpečení je často mizerné a v řadě případů nemáte jako uživatel ani šanci to změnit. I pro průměrného hackera je pak poměrně jednoduché takové zařízení přes internet ovládnout, což může v lepším případě vést k tomu, že vám uvaří čaj jindy, než jste si přáli, v horším případě díky tomuto přístupu pozná vaše každodenní návyky (např. zjistí, kdy odcházíte do práce a kdy určitě nejste doma). Také ale může učinit z vaší konvice součást botnetu a v nejhorším případě nechá konvici trvale zapnutou a zapálí vám dům.

Tak jako se před majiteli smart zařízení otevírají netušené možnosti jejich využití, stejně **nekonečné jsou i způsoby, jakými se dají zneužít**. A je přitom jedno, zdali zařízení zneužije neznámý hacker, výrobce, stát, anebo zhrzený bývalý milenec.

Některá rizika smart homes

Jistým **průkopníkem v zavádění toho, čemu začínáme říkat smart homes, byly hotelové řetězce**. Ty často umožňují ovládat řadu zařízení a služeb skrze jednotnou platformu, většinou nainstalovanou chytrou televizi. Ta kromě běžného přístupu na internet umožňuje také ovládat zařízení v pokoji (např. světla), objednávat jídlo či jiné služby, kontrolovat svůj hotelový účet, provádět videokonference atd. A byly to právě hotelové řetězce, které zaznamenaly první pokusy o kybernetické ovládnutí těchto zařízení. Hosté drahých hotelů jsou totiž často úspěšní byznysmeni a politici, kteří jsou ideálním cílem pro zloděje a podvodníky, špiony či novináře. Navíc nelze vyloučit, že v případě některých zemí jsou tato zařízení v hotelích zranitelná záměrně. Pokud chcete vědět, co dělá ve svém hotelovém pokoji např. německá kancléřka, stačí se při její návštěvě v hotelu nabourat do chytré televize na stěně hotelu a zapnout bez jejího vědomí mikrofon či videokameru. Člověk ale nemusí být zrovna světový státník, stejná rizika se vztahují i na běžné domácnosti.

„Chytrá“ zařízení mohou přinášet skutečně velké množství bezpečnostních problémů, zde zmíníme ty nejdůležitější. Zřejmě **nejzákladnějším rizikem je možná ztráta soukromí a hrozba zneužití citlivých nebo osobních dat**. Typický smart home bude totiž vybaven velkým množstvím různých senzorů (teploty, světla, pohybu, tlaku atd.), které budou shromažďovat a ukládat velké množství informací. Tyto informace mohou být velmi užitečné pro usnadnění vašeho života a přizpůsobení chodu domácnosti vašim potřebám, znamenají ale také doslova studnici velmi detailních poznatků o vašich každodenních činnostech, zvycích a preferencích (ale také třeba o zdravotním stavu), které se mohou ocitnout v nepovolaných rukou. **Hlavním problémem je, že si v případě smart zařízení často ani neuvědomujeme (či nezjistíme), jaká všechna data vlastně shromažďují, kam se ukládají a jak se dají zneužít**. Při pořízení takového zařízení je proto dobré se nad takovými věcmi zamyslet.

Zřejmě nejčastější formou zneužití těchto informací může být **sběr dat soukromými společnostmi** za účelem personalizace marketingu a zacílení reklamy a služeb. Řada případů svědčí o tom, že k tomu dochází již dnes – v roce 2013 např. britský blogger odhalil, že chytré televizory jisté společnosti vysílají do firmy nezakódované informace o diváckých návycích zákazníků (např. na jaký typ pořadů se nejčastěji dívají, v kterou hodinu sedí obvykle u televize atd.), a dokonce přenášejí i jména souborů na externích USB discích, které do televize vložíte (zřejmě za účelem monitoringu filmového a hudebního pirátství). Takové aktivity jsou jistě značným narušením soukromí, je ovšem nutné si uvědomit, že **zákazník dává často s těmito praktikami společnostem souhlas ve smluvních podmínkách** (které ovšem čte jen velmi málo lidí).

Je dobré si vždy ověřit, že výrobce či dodavatel vaše data tímto způsobem nezneužívá, a zvláště pak se ujistit, že je bez Vašeho vědomí neposkytuje třetím stranám. **V řadě případů je přitom zabezpečení otázkou správného nastavení přístroje**. Obecně platí, že se riziko zvyšuje s vyšším počtem externích připojení, anebo v případě, že **jsou data ukládána na nezabezpečeném či neznámem místě**.

Co je to „war driving“

Obecný problém všech zařízení s přístupem na internet je zabezpečení jejich připojení, které je stále častěji řešeno bezdrátově. Jednou z metod jak takové připojení zneužít, je tzv. war driving, kdy útočník projíždí či prochází čtvrtí města a hledá nezabezpečené bezdrátové připojení (wi-fi, bluetooth). Využívá přitom faktu, že signál často sahá až za hranice domu či pozemku. Pokud narazí na nechráněnou síť (např. bez hesla nebo se slabým heslem) může se v lepším případě jen připojit na váš internet, v horším ale může sledovat veškerý provoz na síti, případně ji použít jako bránu k nainstalování malware. Většina smart zařízení v „chytrých“ domácnostech komunikuje právě bezdrátově se širokým dosahem, a proto jsou vůči war driving velmi zranitelné.

Citlivá data může shromažďovat také stát. V demokratických společnostech s rozvinutým právním systémem existují přísná pravidla pro případné narušování soukromí občanů, třebaže některé zahraniční události (např. aféra Snowden) tyto jistoty zpochybňují. Ne všechny státy jsou ale demokratické a řada z nich přistupuje velmi benevolentně ke šmírování vlastních občanů, případně cizinců (a nejen těch, kteří právě pobývají na jejich území). **Smart zařízení také mohou být rovnou vyrobena se „zadními vrátky“ (backdoor)** za účelem pozdější špionáže – tyto problémy byly často zmiňovány u výrobků čínské provenience. Fenomén smart homes otevře v budoucnu bezpochyby nové právní otázky, které bude možná nutné řešit i legislativní cestou tak, aby skrze tato zařízení nedocházelo k porušování základních občanských práv.

Velké množství dat, které smart zařízení shromažďují, může být stejně tak **lákavé pro zloděje, který se přesně dozví, kdy nebýváte doma, případně si skrze kybernetický útok váš dům rovnou odemkne**. Stejně tak ale může tato data zneužít váš soused, se kterým nemáte nejlepší vztahy. Po informacích z vašeho soukromí mohou toužit novináři (zvláště v případě celebrit či politiků), data ze smart zařízení mohou být také skvělým zdrojem informací pro voyeury a sexuální stalkery. Mohou je zneužít dokonce i členové vaší vlastní domácnosti (např. děti proti rodičům či naopak, manžel ke špehování manželky atd.). **Proto je nutné věnovat pozornost zabezpečení přístupů k těmto datům a zamyslet se jakým způsobem by bylo možné je zneužít**.

Problémem řady smart zařízení je to, že jejich **výrobci věnují zabezpečení mnohdy minimální pozornost**. Fenomén IoT se dynamicky rozvíjí a nemalý podíl na něm mají malé (často doslova „garážové“) firmy a start-upy, které se pokouší prorazit se zajímavým praktickým nápadem, ale na vývoj či implementaci pokročilejšího zabezpečení buď nemají peníze či znalosti, anebo tento aspekt zcela ignorují. Taková snaha ušetřit se pochopitelně může týkat i velkých firem. Nemalá řada z takových nových zařízení tak **citlivá data přenáší bez jakéhokoliv šifrování, neumožňuje změnu defaultního hesla, nepoužívá žádné antivirové řešení či firewall, obsahuje četné bezpečnostní zranitelnosti atd.** V současnosti je navíc běžné, že se v jedné domácnosti potkávají nejrůznější zařízení od různých výrobců, jejichž zabezpečení nemusí být navzájem zcela kompatibilní a např. malware se může skrze jednotnou platformu rozšířit z jednoho zařízení na druhé.

Přitom **tato zařízení mohou při útoku nebo nesprávném používání způsobit doslova „fyzické škody“** (např. dálkové ovládání plynových kotlů, rozvodů vody atd.). Ostatně nemusí jít ani o útok, bohatě stačí např. porucha či výpadek proudu. Pokud máte např. elektronické ovládání veškerých zámků v domě (což je dnes např. v USA stále běžnější), může vás výpadek proudu doslova uvěznit uvnitř, anebo vám nedovolí se dostat domů (případně naopak otevře váš dům každému kolem). Pokud máte veškerá data a dokumenty v jednotném media centru, které je ukládá do cloudu, pak se k nim v případě výpadku internetového připojení zkrátka nedostanete. Na to vše je nutné pamatovat zejména

proto, že smart systémy (ať už se jedná např. o ledničky či vytápění) jsou obvykle mnohem složitější než běžná zařízení stejného typu, přičemž **složité systémy mají obecně větší náchylnost k chybě či k poruše. Vůbec nejčastěji pak k takovým situacím dochází nesprávným používáním.**

Pokud se někomu cizímu podaří skrze kybernetický útok ovládnout media centrum, ze kterého kontrolujete veškerá svá smart zařízení, může to znamenat opravdu velký problém (viz rámeček o war driving). Takovým **centrálním bodem přístupu často bývá např. mobilní telefon – při jeho kompromitaci, získáte přístup ke všem jeho funkcím, včetně ovládání smart zařízení v domácnosti**. Možností, které se takovému útočníkovi nabízí, je celá řada. Kombinace dat z více zařízení dá i cizímu člověku překvapivě komplexní obrázek o vašem každodenním životě. **Získaná data je možné použít k vydírání či s nimi obchodovat.** Útočník může tímto způsobem svou oběť šikanovat (např. uprostřed noci zapínat světla, pouštět hlasitou hudbu či vypínat vytápění), sexuálně ji obtěžovat či vyhrožovat. Může ji ve vhodnou chvíli donutit opustit dům, či jí naopak nedovolit přístup do domu, případně k některým důležitým zařízením v domě. Poměrně snadné (a v podstatě nevyžadující žádné znalosti IT) je i **vzdálené rušení veškerého bezdrátového provozu** v domě (např. ze sousedního domu či z jeho okolí), což může v případě, že je většina vašich přístrojů ovládána dálkově, představovat značný problém. Vaše domácí zařízení lze vyřadit také poměrně jednoduchým DDoS útokem (případně je naopak k DDoS útoku využít).

Skrze některá zařízení můžete také platit kreditní kartou (např. výše zmíněná lednička), což pochopitelně zvyšuje riziko zneužití vašich financí. Při útoku na smart domácnost **může útočník získat údaje o vašich platebních kartách, číslech účtů, proběhlých platbách a objednávkách atd.** Útočník může peníze buď přímo odcizit, anebo jen využít získané informace k provedení velmi cíleného podvodného útoku (např. metodou spear phishingu atd.). **Informace lze využít také k získání fyzického přístupu do domu**, např. na dálku rozbít některé zařízení a vzápětí vás navštívit a vydávat se za opraváře, případně přijít oblečen jako kurýr pět minut poté, co jste si objednali nějakou zásilku (v takovém případě prakticky každý otevře domovní dveře). Díky informacím získaným z vašich smart přístrojů vás může daleko snadněji podvést podomní prodavač či obecně kdokoliv s kým uzavíráte nějaký kontrakt či smlouvu. **Útočník může také manipulovat s informacemi, které máte uložené, pozměňovat je či mazat.** Může z vašich zařízení provádět platby, stahovat či poskytovat ilegální obsah, případně si přivlastnit vaši identitu a využít ji při páchání trestné činnosti.

Ke všem smart zařízením je zkrátka nutné přistupovat jako ke klasickým stolním počítačům a používat přinejmenším takové standardy zabezpečení, jako o běžných PC. I váš vysavač či mikrovlnná trouba budou brzy vystaveny potenciálnímu napadení počítačovým virem či jiným kybernetickým útokem a je třeba se proti tomu umět bránit. Problém je často v tom, že tato zařízení ani nemají displej či přístupné uživatelské rozhraní, které by majiteli umožňovalo jejich zabezpečení upravit či kontrolovat. To může vést k tomu, že případný útok může zůstat neodhalen po velmi dlouhou dobu.

Několik doporučení pro zacházení s „chytrými“ zařízeními

- **Čtěte návody a manuály.** V řadě případů dochází k narušení bezpečnosti přístrojů jejich nesprávným používáním či nastavením. Řada zařízení umožňuje individuální nastavení zabezpečení či ochrany soukromí (podobně jako např. Facebook). Věnujte tedy správnému nastavení pozornost. Pokud to zařízení umožňuje, proveďte hned po jeho zakoupení změnu defaultního přístupového hesla a zvolte nové podle pravidel pro tvorbu „silného“ hesla.

- **Věnujte pozornost nastavení přístupů k datům či k ovládání jednotlivých prvků**. Řada zařízení umožňuje mít více přístupových účtů chráněných heslem, na kterých lze nastavit různá oprávnění. To je důležité např. pro přístup dětí či cizích návštěvníků domu. Porucha či výpadek proudu může také způsobit ztrátu důležitých dat, je proto vhodné je **pravidelně zálohovat**.

- **Nespoléhejte stoprocentně na „chytrá“ zařízení** a buďte připraveni na případnou poruchu či výpadek proudu.

- **Čtěte smluvní podmínky výrobců a dodavatelů těchto zařízení.** Často je zde uvedeno, jakým způsobem **může přístroj narušovat vaše soukromí a shromažďovat některá data (případně je poskytovat třetím stranám)** a také, že jeho pořízením dáváte s těmito praktikami souhlas. Pokud Vám některé formulace nejsou jasné, obraťte se na svého prodejce či přímo na výrobce. Pokud s podmínkami nesouhlasíte, vyberte si přístroj od jiného dodavatele. Pokud máte důvodné podezření, že přístroj nezákonně umožňuje přístup k Vašim citlivým datům, aniž byste dali k takové činnosti souhlas, můžete na tuto skutečnost upozornit úřady.

- Varování, která budou uvedena v této kapitole, se v žádném případě netýkají všech smart zařízení, která jsou nebo budou dostupná. V současné době se vývoji a prodeji v rámci tzv. internetu věcí věnuje velké množství firem a celkově lze říci, že **úroveň bezpečnosti jednotlivých zařízení je velmi nevyrovnaná**. **Věnujte proto pozornost výběru správného dodavatele** těchto zařízení a zjistěte, jaký poskytuje následný servis a pomoc při potížích, případně zda aktualizuje svůj software v reakci na bezpečnostní hrozby.

- **Řada doporučení pro smart homes je obecně shodná s pravidly pro bezpečné používání mobilních zařízení**. Řadu z nich naleznete v jednom z předchozích vydání této situační zprávy, kde byl této problematice věnován delší exkurz (situační zpráva za 2. pololetí 2013).

Vybrané události ve sledovaném období

Červenec

Mezinárodní akce proti malwaru Shylock

Ve dnech 8. – 9. července se uskutečnila rozsáhlá mezinárodní operace za účelem ochromení internetových domén a serverů, ze kterých byl provozován úspěšný trojský kůň Shylock. Jméno malware dostal podle toho, že lze v jeho zdrojovém kódu nalézt na několika místech citace ze Shakespearova Kupce benátského. Tím ale veškerá jeho poetika končí – tomuto trojskému koni se podařilo okrást o data i o peníze tisíce lidí. Virus cílil především na internetové bankovnictví. Celkem napadl nejméně 30 tisíc zařízení, převážně ve Velké Británii.
Během akce se podařilo rozbít síť zařízení a systémů, na kterých byl Shylock provozován. Operaci vedla britská NCA (National Crime Agency), zapojilo se do ní ale řada partnerů ze soukromé i veřejné sféry, včetně Europolu, FBI, firem BEA Systems, Dell, Kaspersky Lab a britské zpravodajské služby GCHQ. Vyšetřování probíhalo z operačního centra EC3 v Haagu a podílely se na něm i italské, nizozemské, polské a turecké orgány.

Srpen

Největší krádež hesel v historii internetu?

V průběhu srpna 2014 mělo dojít k obřímu hackerskému útoku na více než 420 tisíc internetových stránek a FTP serverů, který provedla skupina nazývaná experty jako CyberVor (kyberzloděj). Tomuto gangu se mělo podařit ukrást více než 1,2 miliardy hesel do různých služeb, což společnost Hold Security označila za největší krádež přihlašovacích údajů v historii internetu. Postiženými byly jak velké firmy, tak ale i malé či dokonce osobní webové stránky. Zacílení hackerů bylo tedy velmi široké, hackeři se zjevně snažili vybudovat si obří databázi hesel. Některá nakupovali i na černém trhu od jiných hackerských skupin. CyberVor hesla využíval k šíření spamu i k infikování systémů škodlivými kódy. Není jasné, jak moc byli útokem zasaženi čeští uživatelé internetu.

Vládní CERT akreditovaným členem sdružení Trusted Introducer

Vládní CERT (GovCERT.CZ) je od 21. srpna 2014 akreditovaným členem Terena-Trusted Introducer. Sdružení Trusted Introducer (TI) působí v rámci evropské organizace TERENA a sdružuje evropské bezpečnostní týmy vládní, národní, komerční sféry (např. bank, provozovatelů internetového připojení, výrobců hardware ad.) nebo univerzit. Vstup vládního GovCERT.CZ mezi akreditované týmy TI znamená další krok k užší spolupráci se světovou infrastrukturou bezpečnostních týmů CERT nebo CSIRT a zvýšení prestiže na mezinárodní scéně. Jedná se o placené členství, z něhož mj. vyplývá přístup k celé řadě informací a kontaktů v partnerských evropských zemích.

Září

Úspěšný zásah jihomoravských kriminalistů proti nebezpečnému hackerovi

Jihomoravským kriminalistům z Oddělení informační kriminality se podařilo objasnit případ, který je v rámci celé České republiky mimořádným svým rozsahem i technickou sofistikovaností. Na rozpletení případu a dopadení pachatele pracovali kriminalisté dva roky a na podzim 2014 zahájili trestní stíhání šestatřicetiletého muže z Brněnska pro trestné činy neoprávněný přístup k počítačovému systému a nosiči informací a opatřování a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat.

Vyšetřování bylo zahájeno na základě upozornění bezpečnostního týmu CSIRT-MU Masarykovy univerzity. Dosud netrestaný muž nejméně od roku 2007 neoprávněně překonával bezpečnostní opatření počítačových systémů, a to nejen na území České republiky, ale i v cizině. Poté, co se tímto způsobem do počítače naboural, získal administrátorská oprávnění a dostal se tak nejen k datům uloženým v zařízení, ale i k přihlašovacím údajům všech uživatelů, kteří se k tomuto systému následně přihlásili. K tomuto využíval škodlivého software, který sám vytvořil. Přístupové údaje těchto uživatelů si neoprávněně ukládal, aby je v budoucnu mohl použít k napadení dalších počítačových systémů. Tímto způsobem překonal bezpečnostní opatření u nejméně 1500 počítačů fyzických i právnických osob s převážně linuxovými operačními systémy, nad kterými díky tomu měl plnou kontrolu, včetně zkopírování firemní i soukromé e-mailové pošty. Podle slov kriminalistů, kteří případ vyšetřují, dosud podobně rozsáhlý útok žádný policejní orgán v republice nešetřil. Případ je mimořádný jak enormním počtem napadených počítačů, tak i sofistikovaností a technickou vyspělostí metod, které pachatel k této činnosti používal. Vyšetřovatelé při složitém pátrání po pachateli spolupracovali primárně s odborníky z bezpečnostního týmu CSIRT-MU Masarykovy univerzity v Brně a dále s brněnskou Fakultou informačních technologií Vysokého učení technického a sdružením CESNET. K objasnění tohoto komplikovaného případu přispěla jak velmi dobrá spolupráce s těmito institucemi, tak i fakt, že na jihomoravském policejním ředitelství funguje specializovaný útvar kriminalistů zabývající se vyšetřováním informační kriminality.

Obviněný muž se k trestné činnosti doznal, v případě odsouzení mu hrozí trest odnětí svobody v trvání dvou let. Výše hrozícího trestu se však ještě může změnit dle výsledků dalšího vyšetřování. Jedním z jeho cílů je také objasnění hackerova motivu a zejména pak způsob následného využití neoprávněně získaných dat.

Odborný seminář Policejního prezidia ČR a Europolu

Čtyřicet procent lidí na světě je online, již v roce 2017 by to pak měla být polovina celosvětové populace. Nedávné renomované odhady vyčíslují globální škody způsobené internetovou kriminalitou na částku přibližně 300 miliard dolarů ročně. Právě k aktuálním trendům v oblasti internetové kriminality uspořádalo Policejní prezidium ČR a Europol odborný seminář, který se uskutečnil 19. září 2014 v rámci Dnů NATO v Ostravě. "Chceme zhodnotit zkušenosti s počítačovou kriminalitou na mezinárodní úrovni a sjednotit postupy v boji proti tomuto novodobému kriminálnímu fenoménu," uvedl policejní prezident Tomáš Tuhý ve svém zahajujícím projevu.

Tato aktivita má návaznost na předešlé setkání policejních prezidentů okolních zemí v rámci téže akce v minulém roce, na kterém se zúčastnění shodli na potřebě intenzivního řešení této oblasti. "Kriminalita v kybernetickém prostředí úzce souvisí s kybernetickou bezpečností na jedné straně a hrozbami kybernetických útoků, které mají vojenský charakter, na straně druhé. V tomto ohledu je pak nutné postupovat jednotně a je nutné současně řešit kybernetickou bezpečnost, obranu i kriminalitu," doplnil policejní prezident. Z tohoto důvodu si vytyčil potírání internetové kriminality jako jednu ze svých priorit. Také tato akce je důkazem zvyšování efektivity a práce Police ČR v dané oblasti.

Na odborném semináři se diskutovalo o otázkách aktuálních trendů v oblasti informační kriminality, i o řešení struktury organizace boje s tímto druhem kriminality. Odborníci dále otevírali témata problematiky virtuálních měn, spolupráce s veřejností, sociálních sítí, kybernetické bezpečnosti, kyberterorismu, útoků na kritickou a významnou infrastrukturu a další. Zastoupení účasti mezinárodního odborného semináře bylo široké - od významných představitelů okolních zemí zabývajících se kriminalitou v prostředí informačních technologií, přes specialisty Evropského centra kyberkriminality (EC3), národních představitelů zodpovědných za kybernetickou bezpečnost, až po specialisty orgánů činných v trestním řízení, a to jak z řad policie, tak ze státního zastupitelství.

Říjen

2. společná konference Europolu a Interpolu k informační kriminalitě

Identifikovat nové hrozby a trendy v informační kriminalitě měla za cíl v pořadí druhá konference k informační kriminalitě, kterou společně pořádaly Interpol a Europol, a která se konala ve dnech 1. – 3. října 2014 v Singapuru. Dohromady se na ní sešlo přes 230 specialistů z řad bezpečnostních a státních složek, soukromého sektoru i akademiků. Účastníci byli z celkem 55 zemí. Hojně diskutováno bylo praní špinavých peněz skrze online sázení, ale také rizika virtuálních měn a nové možnosti digitální forenzní analýzy. Velká pozornost byla věnována diskusi jak útočníky nejen odhalit, ale také u soudu usvědčit, zejména ve chvíli, kdy je případ vyšetřován paralelně v několika zemích.

Říjen jako měsíc kybernetické bezpečnosti

V říjnu 2014 opět proběhla celoevropská kampaň s názvem Evropský měsíc kybernetické bezpečnosti (ECSM), koordinovaná Evropskou agenturou pro síťovou a informační bezpečnost (ENISA) a DG CONNECT Evropské komise. Cílem kampaně je podpořit osvětu v oblasti kybernetické bezpečnosti. V České republice je kampaň ECSM koordinována Národním centrem bezpečnějšího internetu a probíhá pod záštitou Mgr. Vladimíra Rohela, ředitele Národního centra kybernetické bezpečnosti, a záštitou JUDr. Miroslava Antla, předsedy Ústavně-právního výboru Senátu Parlamentu ČR. Více informací o akcích, pořádaných v rámci této každoroční kampaně, lze nalézt na stránkách www.saferinternet.cz a www.cybersecuritymonth.eu.

EVROPSKÝ MĚSÍC KYBERNETICKÉ BEZPEČNOSTI

Virus Reign špehoval 7 let bez povšimnutí

Společnost Symantec odhalila nový spyware, který mohl být využíván ke špehování soukromých společností, vládních institucí i jednotlivců. O jeho sofistikovanosti svědčí to, že byl spuštěn již v roce 2008, odhalen byl ale až na podzim 2014. Virus dokáže pořizovat (a svému původci šifrovaně odesílat) v pravidelných intervalech snímky obrazovky, krást hesla, a dokonce obnovit smazané soubory. Útočníci se tak mohou dostat i k datům, která sám uživatel považoval za dávno neexistující.

Není přitom jasné, jaká data virus vlastně sbíral a k čemu byla zneužívána. Nejvíce postižených počítačů bylo v Rusku, Irsku a Saúdské Arábii, záběr malwaru byl ale globální a byl odhalen i v mnoha dalších zemích (výskyt v České republice nebyl prozatím potvrzen). Stopy tentokrát nevedou do východní Evropy, ale spíše na Západ – k této variantě se přiklánějí bezpečnostní experti, kteří virus analyzovali. Objevily se i spekulace o autorství některé ze zpravodajských služeb, ty ale nelze nijak potvrdit.

Cvičení CYBER EUROPE 2014

Více než 200 organizací a 400 odborníků na kybernetickou bezpečnost z 29 evropských zemí si v říjnu vyzkoušelo svou připravenost k zásahu proti počítačovým útokům při celodenní simulaci, kterou zorganizovala Evropská agentura pro bezpečnost sítí a informací (ENISA). V průběhu cvičení Cyber Europe 2014 odborníci z veřejného i soukromého sektoru, včetně agentur pro kybernetickou bezpečnost, vnitrostátních skupin pro reakci na počítačové hrozby, ministerstev, telekomunikačních firem, energetických společností, finančních institucí a poskytovatelů internetových služeb, testovali své postupy a kapacity v rámci realistického a rozsáhlého scénáře ohrožení kybernetické bezpečnosti.

Cyber Europe 2014 je největší a nejkomplexnější cvičení na toto téma pořádané v Evropě. Řešilo více než 2 000 jednotlivých kybernetických incidentů, mimo jiné DoS útoky (přehlcení internetových služeb), informace zpravodajských služeb a sdělovacích prostředků o kybernetických útocích, útoky měnící vzhled webových stránek (tzv. defacement), krádeže citlivých informací, útoky na kritickou infrastrukturu, jako jsou energetické nebo telekomunikační sítě, a testování postupů spolupráce a eskalačních postupů EU. Jedná se o cvičení rozložené mezi několik testovacích středisek v celé Evropě, která jsou koordinována centrálním kontrolním střediskem. O zapojení České republiky do tohoto cvičení více v sekci „Aktivity ČR v oblasti kybernetické bezpečnosti“ této kapitoly situační zprávy.

Listopad

K boji Europolu proti informační kriminalitě se připojuje Norsko

11. listopadu 2014 bylo podepsáno Memorandum o porozumění mezi Evropským centrem informační kriminality (EC3) a jeho norskou obdobou – Centrem pro kybernetickou a informační bezpečnost (CCIS). Obě instituce tak budou sdílet řadu informací a vzájemně kooperovat při potírání online kriminality. Ačkoliv tak Norsko není členem EU, jednoznačně vnímá, že informační kriminalita nebere na žádné politické hranice ohled. Spolupracovat bude i norský národní CERT. K iniciativě se připojilo i 25 norských soukromých společností podnikajících v rámci služeb informační společnosti, to vše v rámci kooperace veřejného a soukromého sektoru.

Odhalena kritická chyba u zařízení Apple

Experti společnosti FireEye popsali závažnou bezpečnostní zranitelnost u chytrých telefonu iPhone a tabletu iPad od společnosti Apple. Podle FireEye se jedná o vůbec největší bezpečnostní trhlinu v historii zařízení od této firmy. Mohla být zneužita k odcizení citlivých dat z přístrojů (fotek či videí, ale také přihlašovacích údajů do internetového bankovnictví či emailu) nebo k jejich ovládnutí. Odhalení chyby je také důležité pro zboření mýtu, který koluje mezi některými fanoušky Applu, že zařízení od této firmy se viry a zranitelnosti netýkají (podobné to bylo např. s uživateli operačního systému Linux). Ve skutečnosti je nutné dodržovat základní bezpečnostní pravidla bez ohledu na výrobce zařízení.

FireEye nakonec chybu zveřejnil ve chvíli, kdy internetem začaly kolovat první viry, snažící se o její zneužití. Výrobce byl přitom informován ještě před tímto zveřejněním. Problém se týkal všech zařízení, na kterých byl nainstalován iOS ve verzích 7.1.1, 7.1.2, 8.0, 8.1 a 8.1.1 beta. Důvodem existence této bezpečnostní chyby je, že systém iOS si při aktualizaci aplikace se stejným identifikátorem nevyžádá odpovídající certifikát, jenž by dokazoval, že aktualizace pochází z důvěryhodného zdroje. V zásadě tedy útočníkům stačí zadat malwaru stejný identifikátor, jako má původní aplikace z AppStoru. Tímto způsobem může být nahrazena libovolná aplikace z oficiální nabídky, výjimkou jsou pouze systémové, v telefonu napevno nainstalované aplikace (Safari, fotoaparát, přehrávač apod.). Malware zcela nahradí původní aplikaci včetně ikony, i nadále se přitom bude tvářit stejně. V současné době by měla již být k dispozici bezpečnostní záplata, důležité jsou proto pravidelné aktualizace operačního systému.

Mezinárodní akce proti nelegálním internetovým tržištím v síti Tor

Operační centrum Evropského centra informační kriminality v Haagu koordinovalo operaci 16 evropských zemí a USA proti několika „dark markets“, provozovaných jako skryté služby v síti Tor. Operace s názvem „Onymous“ cílila na servery, na kterých docházelo mj. k prodeji zbraní a drog (fenoménu ilegálních internetových tržišť a virtuálních měn byl věnován rozsáhlejší exkurz v minulé situační zprávě). Akce skončila zatčením 17 osob (provozovatelů tržišť a obchodníků), z provozu bylo vyřazeno 410 různých skrytých služeb, včetně reinkarnace slavné „Hedvábné stezky“ (Silk Road 2.0). Zadrženy byly také bitcoiny v hodnotě 1 milionu dolarů, 180 tisíc EUR v hotovosti, ale také drogy, zlato a stříbrné šperky. Akci podporoval také nový štáb J-CAT (Joint Cybercrime Action Taskforce), který vznikl teprve v září 2014. Právě J-CAT má sloužit jako platforma pro podobné logisticky a koordinačně náročné operace, které cílí na kybernetické kriminální sítě a infrastrukturu. Česká republika byla jednou ze zúčastněných zemí.

Česká pošta varovala před podvodnými emaily

Další velká vlna podvodných emailů, které se vydávají za zprávy od České pošty, se začala ČR šířit v říjnu. Podvodné e-maily jsou psány ve formě „Informace o Vaší zásilce", kde najde klient údaje o nedodání zásilky a odkaz pro stažení informací o zásilce, který již vede na podvodnou webovou stránku. Pošta varovala klienty, aby v žádném případě neklikali na žádný z odkazů, uvedených v takovém emailu a o nebezpečném mailu dali vědět na adresu info@cpost.cz. Emaily jsou rozesílány z adres, které sice České poště nepatří, ale její oficiální adresu připomínají např. cpost@cs-post.net nebo zasilka@cs-post.net.

V tomto případě vedl odkaz v mailu k nákaze klasickým ransomware. Po kliknutí byli uživatelé přesměrováni na falešné stránky České pošty, kde si mohli stáhnout soubor ve formátu ZIP s přiloženým EXE souborem. Ten zašifruje všechny dokumenty na disku a požaduje výkupné za jejich odemknutí. Ani lidé, kteří výkupné zaplatili, ovšem klíč ke svým datům nezískali. Na rozdíl od pokročilejších ransomware bylo ale v tomto případě možné počítač odborným zásahem malwaru zbavit. Nejde přitom o první vlnu šíření podobných emailů v Česku – v minulé situační zprávě jsme informovali o případu ženy z Kroměřížska, která podobným způsobem přišla o 400 tisíc Kč. Tehdy email hrozil nesplaceným dluhem a snažil se získat údaje k internetovému bankovnictví.

ČR a Izrael podepsaly prohlášení o spolupráci v oblasti kybernetické bezpečnosti

Česká republika a Stát Izrael s odkazem na dlouhodobé historické vztahy a společné zájmy obou zemí a s ohledem na aktuální kybernetická bezpečnostní rizika v listopadu v Jeruzalémě podepsaly Společné prohlášení o spolupráci mezi vládou ČR a vládou státu Izrael v oblasti kybernetické bezpečnosti. Zástupci obou stran se dohodli na těchto ustanoveních zmíněného prohlášení:

- sdílení informací, osvědčených postupů a zkušeností týkajících se kybernetických bezpečnostních hrozeb a událostí, jakož i jiných relevantních otázek týkajících se kybernetické bezpečnosti,
- zvýšení celkové kybernetické odolnosti a připravenosti proti internetovým hrozbám prostřednictvím sdílení informací, výměnou zkušeností a spolupráce v odborné přípravě včetně společných kybernetických cvičení,
- sdílení relevantních informací o projektech výzkumu a vývoje v oblasti kybernetické bezpečnosti,
- vytvoření zabezpečeného komunikačního kanálu za účelem sdílení informací týkajících se kybernetických bezpečnostních hrozeb a událostí.

Vzájemná spolupráce přispěje nejen k posílení kybernetické bezpečnosti v obou zemích, ale i k podpoře hospodářské spolupráce a prohloubení kontaktů v oblasti vědy, výzkumu a inovací. Prohlášení podepsali za Českou republiku Jaroslav Šmíd z Národního bezpečnostního úřadu (NBÚ) a za Stát Izrael Eviatar Matania z National Cyber Bureau.

Prosinec

Razie švédské policie proti Pirate Bay

Švédská policie zasáhla proti známému serveru na popud švédské organizace pro boj proti internetovému pirátství Rights Alliance. Ta si stěžovala na údajné porušování autorských práv ze strany Pirate Bay. Naopak švédská Pirátská strana (která v roce 2009 vybojovala také jedno křeslo v Evropském parlamentu) razii kritizovala jako pokus kriminalizovat nediskriminační šíření dat. Krátce po zásahu přestala stránka fungovat.

The Pirate Bay je jedním z největších webů na bezplatné sdílení souborů na světě a miliónům uživatelů nabízí hudbu, filmy i počítačové hry. Již v minulosti byla trojice jeho spoluzakladatelů, včetně v Thajsku zatčeného Hanse Fredrika Lennarta Neije, odsouzena za porušování autorských práv. Po uzavření serveru Megaupload a zatčení jeho zakladatele, známého jako Kim Dotcom, na Novém Zélandu (o této události jsme informovali v minulých situačních zprávách), se jedná o další policejní zákrok proti mezinárodně významnému serveru na sdílení souborů.

Zhruba dva týdny po policejní razii byla doména Pirate Bay opět oživena, místo původního obsahu zde ale bylo možné nalézt jen pirátskou vlajku.

Herní konzole PlayStation a Xbox terčem hackerského útoku

V průběhu vánočních svátků napadli hackeři síťový systém společnosti Sony, který využívá její herní konzole PlayStation. Útok, ke kterému se přihlásila skupina Lizard Squad, jistě pokazil Vánoce v nejedné domácnosti, kde konzole posloužila jako vánoční dárek. Síť Sony se totiž potýkala s několikadenními problémy. PlayStation používá celkem 56 milionů hráčů, řada z nich nemohla během svátků hrát síťové varianty her. Sony byla v roce 2014 terčem hackerů několikrát, ještě větší pozornost vyvolal útok, při kterém unikla citlivá data a hackeři požadovali stažení filmu Interview (který je o atentátu na severokorejského vůdce Kim Čong Una) výměnou za jejich nezveřejnění. U obou útoků se do vyšetřování zapojila FBI.

Stejná skupina zaútočila také na síťový systém od konzole Xbox od společnosti Microsoft, té se ale podařilo problém vyřešit rychleji, takže většina jejích zákazníků žádné výpadky nezaznamenala.

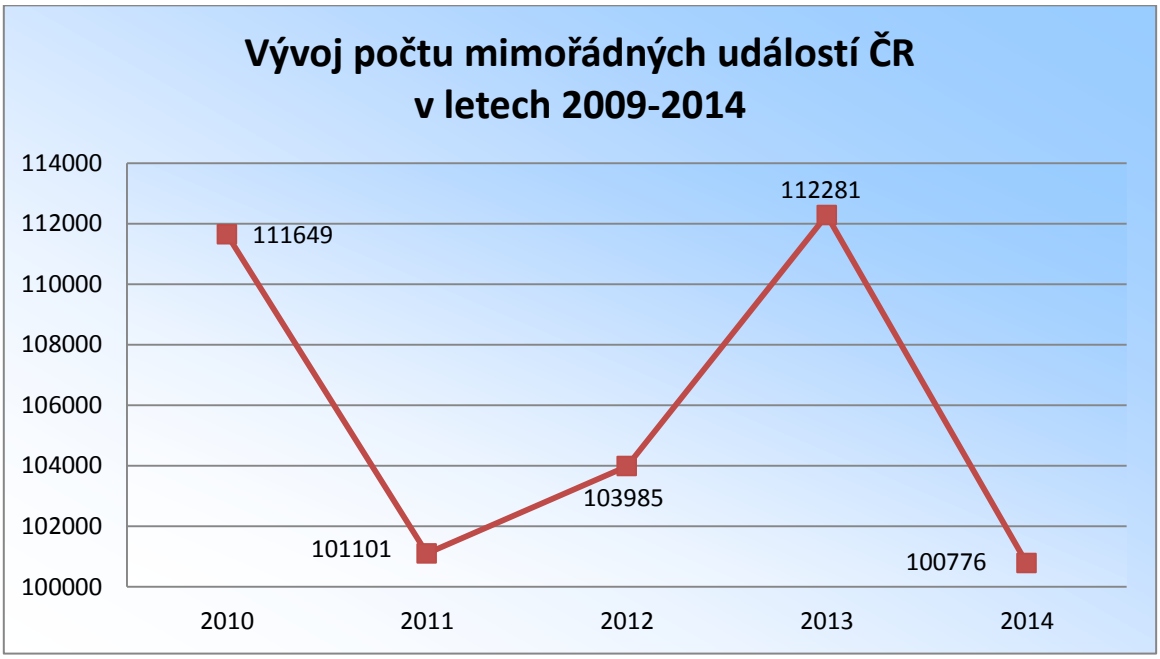
Zdroje pro tuto kapitolu: PČR, NBÚ, ČTK, MZV, sxc.hu, idnes.cz, europol.europa.eu,aphaia.co.uk, allpremium4.blogspot.com, aktualne.centrum.cz, govcert.cz, lidovky.cz, novinky.cz, technet.idnes.cz, zive.cz, e15.cz, trustport.com, csas.cz, kickstarter.com, interpol.int, hpsolutions.cz, economist.com, csoonline.com, edition.cnn.com, enisa.europa.eu, en.wikipedia.org, tomshardware.com, stanford.edu, chip.cz, newscientist.com, russelwebster.com, eset.cz, businessworld.cz, itbiz.cz, infoworld.com, europa.eu computerworld.cz, net-security.org, mcafee.com, itnewsafrica.com, scmagazine.com.au, businessinsider.com, blackhat.com, extremetech.com, umsl.edu, svetaplikaci.tyden.cz, amazongenius.com, tech.ihned.cz, bbc.com, zpravy.aktualne.cz, itnetwork.cz, gstylemag.com, diit.cz, echo24.cz, www.m-journal.cz, cleverandsmart.cz, danielzstinson.wordpress.com, pcworld.com, symantec.com, h30499.www3.hp.com, tech.ihned.cz, ceskenoviny.cz, ec.europa.eu, policie.cz,

KRIZOVÉ ŘÍZENÍ

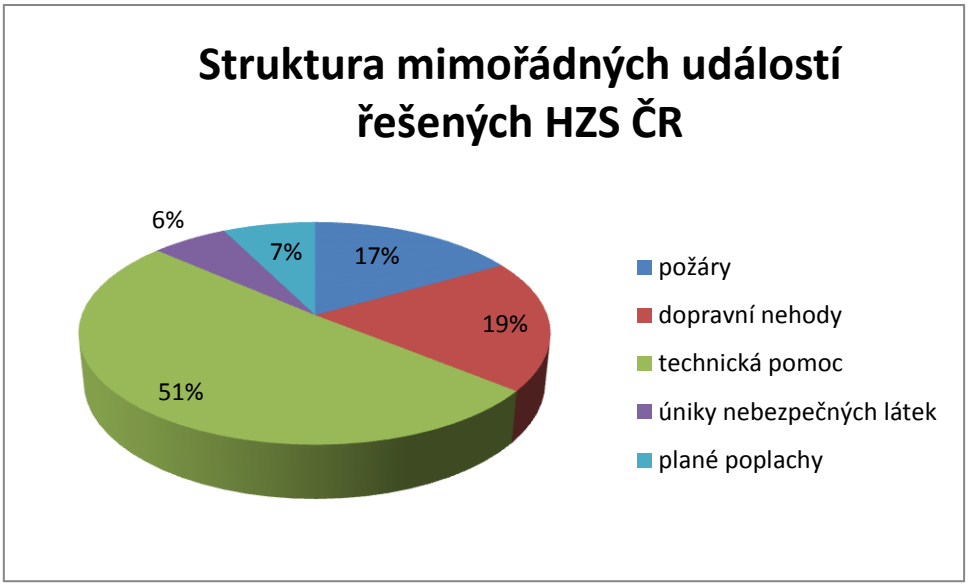
Hasičské statistiky a jejich interpretace

Namísto policejních statistik se v tomto případě soustředíme na statistiky MV - Generálního ředitelství Hasičského záchranného sboru ČR, konkrétně na data za uplynulý rok 2014. Tyto statistické výstupy jsou v podrobnější verzi pravidelně aktualizovány na stránkách www.hzscr.cz.

V roce 2014 zasahovaly jednotky požární ochrany celkem u 100 776 událostí. Z přiloženého grafu je patrné, že se jedná o vůbec nejnižší počet mimořádných událostí za posledních pět let (v této souvislosti je ale nutné říci, že některé, např. výbuch muničního skladu ve Vrběticích, byly poměrně velkého rozsahu). Podařilo se tak zvrátit negativní trend nárůstu incidentů, který bylo možné pozorovat od roku 2011.

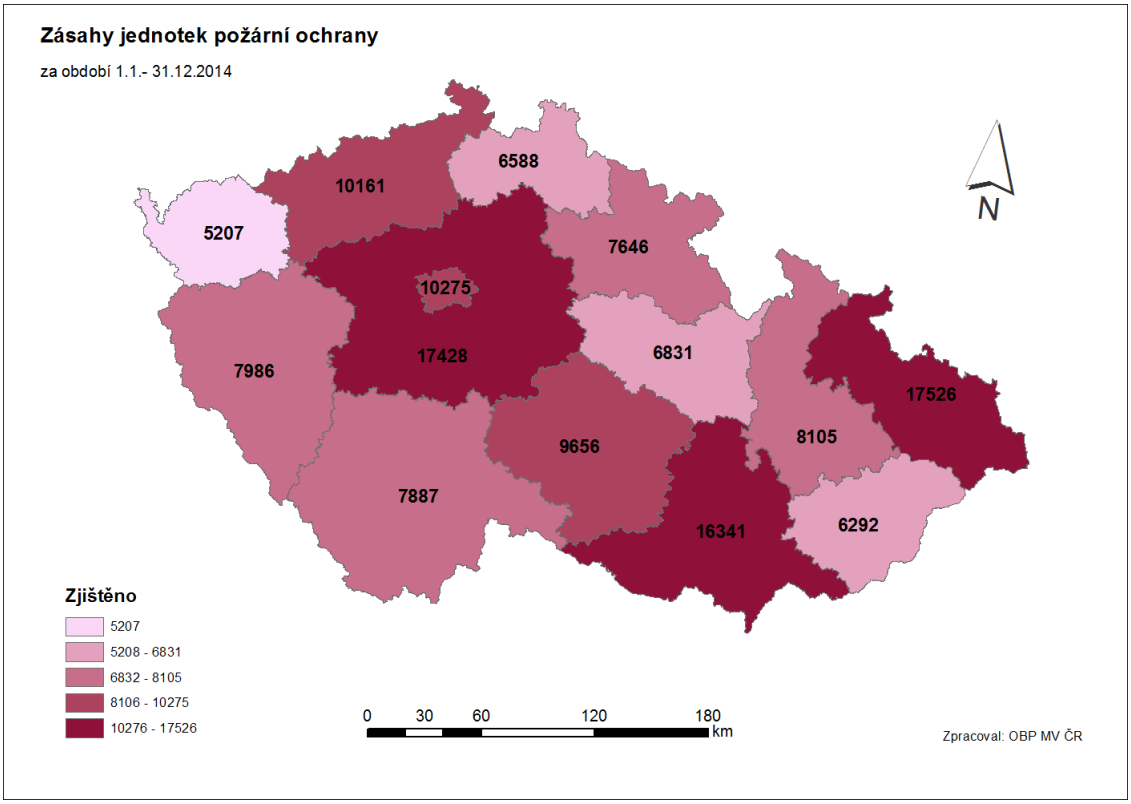


Z hlediska struktury mimořádných událostí **se hasiči v roce 2014 nejčastěji (ve více než polovině případů) podíleli na různých formách technické pomoci**. Zároveň asistovali u 19 219 dopravních nehod a 6 161 úniků nebezpečných látek (z toho se v 4 793 případech jednalo o ropné produkty). V celkem 7 527 případech se jednalo o plané poplachy, což představuje 7,4 % všech výjezdů. Také **počet planých poplachů byl nejnižší za posledních pět let**, naopak počet požárů a dopravních nehod oproti roku 2013 mírně stoupl, třebaže o pouhé jedno resp. dvě procenta. Hasiči nicméně i v roce 2014 vyjížděli častěji k dopravním nehodám než k ohni.



Vůbec **nejrizikovějším krajem v ČR** z hlediska počtu mimořádných událostí zůstává se značným náskokem **Vysočina**, kde na 1000 obyvatel připadá ročně 16 hasičských výjezdů. Následován je krajem Karlovarským s 12,8 výjezdy. Naopak nejméně výjezdů v přepočtu na počet obyvatel bylo zaznamenáno v kraji Zlínském (7) a v Praze (7,2). Největší počet požárů byl naopak zaznamenán v kraji Ústeckém, kde jich bylo v roce 2014 evidováno 2,2 na 1000 obyvatel. Nejlépe na tom v tomto ohledu byl opět kraj Zlínský.

Ještě v minulé situační zprávě si nelichotivý primát kraje s nejvyšším počtem mimořádných událostí udržoval **kraj Moravskoslezský**, ten ale (společně se Středočeským krajem) za rok 2014 zaznamenal vůbec **nejvyšší meziroční pokles** (23 %). Situace se naopak nejvíce zhoršila v Olomouckém kraji, kde došlo k 14% nárůstu, a tento kraj se tak společně s Jihomoravským, Zlínským a Karlovarským staly jedinými, kde počet událostí meziročně neklesl. Geografické rozložení mimořádných událostí přehledně znázorňuje následující mapa:

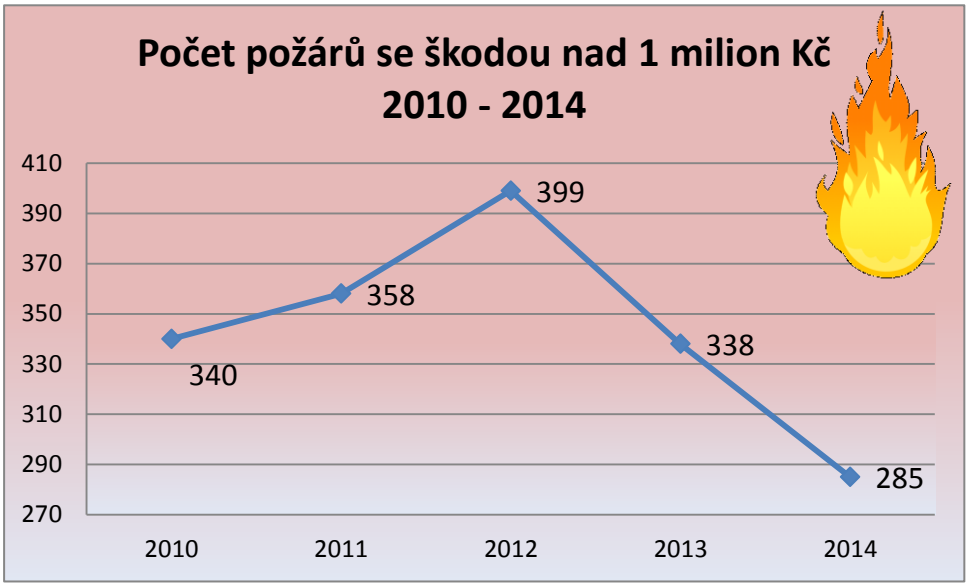


Ačkoliv počet událostí v celkovém součtu klesl, **v případě požárů byl naopak zaznamenán nárůst o 1,4 % oproti roku 2013**. Celkem tedy v ČR za rok 2014 došlo k 17 388 požárům, při kterých **zahynulo celkem 114 osob a 1 179 osob bylo zraněno**.

Celkové škody se vyšplhaly do výše 2 198 327 400 Kč, což je o 8,5 procenta méně, než v roce 2013 (v novém tisíciletí byl v tomto ohledu nejhorší rok 2002, kdy škody přesáhly 3,5 miliardy Kč). Je pozoruhodné, že **za 74 % z celkových škod stojí pouhých 302 největších požárů** (tedy 1,7 % celkového počtu). Některé z nich jsou přehledně zmíněny v závěru kapitoly – zvláštní pozornost je věnována explozím v muničních skladech v areálu Vrbětice, mezi velké události loňského roku ale patřil také např. rozsáhlý požár v kladenských pekárnách, velkou pozornost poutal také požár architektonicky mimořádně cenné horské chaty na Pustevnách.

Ačkoliv částka celkových škod působí astronomicky, je dobré zdůraznit, že díky kvalitě zásahů Hasičského záchranného sboru a dobrovolných hasičů **se podařilo uchránit hodnoty v celkové výši přesahující 11,5 miliardy Kč**. Výše uchráněných hodnot je tedy více 5x vyšší, než výše celkových škod. Zároveň se hasičům podařilo při požárech bezprostředně zachránit 730 osob, dalších 5 963 bylo před požáry evakuováno. V průměru vzniklo v roce 2014 na území ČR denně 48 požárů.

Jelikož o celkových ročních škodách rozhoduje především vývoj počtu velkých požárů (se škodou na 1 milion Kč), je z následujícího grafu patrné, že v tomto ohledu byl uplynulý rok 2014 velmi příznivý.



Rozhodující podíl na spolupráci při zásahu u událostí s jednotkami požární ochrany má **Policie ČR a zdravotnická záchranná služba**. Tyto tři složky tvoří základ IZS. Za rok 2014 bylo evidováno celkem **99 667 zásahů, při kterých došlo k součinnosti** jednotek požární ochrany s ostatními složkami. Nejčastější je spolupráce s Policií ČR (59 508 případů, téměř 60 % celkového počtu), zdravotnická záchranná služba asistovala v 23 132 případech (23 %). Armáda České republiky se na zásazích podílela v 66 případech, například při mimořádné události ve Vrběticích.

Přehled velkých požárů se škodou 20 milionů Kč a vyšší za 2. pololetí roku 2014

3. čtvrtletí 2014

8. 8. – **Požár bývalé továrny na zpracování dřevěné dýhy,**
Kralupy nad Vltavou, okres Mělník
Příčina: nedbalost při lepení izolace pomocí PB hořáku.
Zásah 25 JPO, nutná ochrana nádrže s naftou o objemu 6000 l
Škoda: 30 000 000 Kč.

12. 9. – **Požár kovoobráběcí výrobní haly,** Skuteč, okr. Chrudim
Příčina: technická závada elektrické instalace.
Škoda: 50 000 000 Kč.
Zraněni: 3 hasiči.

12. 9. – **Textilní závod KÜMPERS TEXTIL, spol. s r.o.,**
Těchonín, okr. Ústí nad Orlicí
Příčina: technická závada vzduchového tkalcovského stavu
Škoda: 61 900 000 Kč.
Zraněny: 4 osoby. Evakuováno: 30 osob.

22. 9. – **Operační sál nemocnice,** Frýdek-Místek
Příčina: technická závada nápojového automatu.
Škoda: 29 110 000 Kč.

4. čtvrtletí 2014

21. 12. – **Rekreační lovecká chata,** Dolní Lomná, okr. Frýdek-Místek.
Příčina: v šetření.
Škoda: 22 000 000 Kč.

Přehled připravovaných velkých cvičení pro rok 2015

2015

CMX/CME 2015

- Mezinárodní cvičení orgánů krizového řízení NATO a EU.
- Cvičení by mělo být založena na scénáři operace vedené EU se zapojením sil, prostředků a schopností NATO (Berlin Plus).
- Cvičení má prověřit spolupráci mezi NATO a EU na vojensko-politické úrovni. Účastní se jej členské státy NATO a EU, vybraní partneři a mezinárodní organizace, orgány NATO a EU.
- Doba provedení: 2015

ZDROJE 2016

- Společné vnitrostátní cvičení Správy státních hmotných rezerv, odborné pracovní skupiny Ústředního krizového štábu pro koordinaci zabezpečení věcnými zdroji, KŠ vybraných ministerstev, krajů a obcí s rozšířenou působností.
- Tématem cvičení je vyžadování a poskytování věcných zdrojů za krizového stavu. Cílem je mj. procvičit praktické využívání a funkcionality systému IS KRIZKOM. Cvičení připravuje SSHR, účastní se jej vybraní zaměstnanci SSHR, zástupci vybraných ministerstev a členové krizových štábů.
- Doba provedení: 11. – 12. listopadu 2016.

ROPNÁ NOUZE 2015

- Společné vnitrostátní cvičení Správy státních hmotných rezerv, vybraných krajů a obcí s rozšířenou působností pro řešení krizové situace Narušení dodávek ropy a ropných produktů do ČR.
- Tématem cvičení je řešení stavu ropné nouze, koordinace činností spojených s problémy se zásobováním pohonnými hmotami, včetně zavedení nouzového výdeje pohonných hmot ze správy státních hmotných rezerv. Cvičení připravuje SSHR, účastní se jej vybraní zaměstnanci SSHR, zástupci vybraných ministerstev a členové krizových štábů.
- Doba provedení: 4. čtvrtletí roku 2015.

ZÓNA 2015

- Vnitrostátní vícestupňové cvičení orgánů krizového řízení vybraných ÚSÚ a Jihočeského kraje, vybraných ORP a obcí.
- Cílem je prověřit činnost ÚSÚ, orgánů kraje a dalších subjektů při řešení události vzniklé v souvislosti s havárií na jaderné elektrárně Temelín, prověřit a aktuálnost i reálnost zpracované havarijní dokumentace a systém informování veřejnosti při vzniku radiační havárie.
- Cvičení připravuje MV-GŘ HZS ČR ve spolupráci se SÚJB a MO.
- Předpokládaná doba provedení: 22. – 24. září 2015

Novinky v krizovém řízení v 2. pololetí 2014

Novela nařízení vlády 432/2010 Sb.

Dne 1. ledna 2015 nabylo účinnosti nařízení vlády č. 315 ze dne 8. prosince 2014, kterým se mění **nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury**.

Jak již bylo avizováno v Situační zprávě za 1. pololetí roku 2014, změny se týkají odvětvových kritérií **v odvětví energetiky**, zdravotnictví **a zejména komunikačních a informačních systémů**, kde vzniklo nové „pododvětví“ kybernetická bezpečnost v návaznosti na přijetí zákona č. 181/2014 o kybernetické bezpečnosti a změně souvisejících zákonů (zákon o kybernetické bezpečnosti – více o tomto právním předpisu opět v minulé situační zprávě).

Nově jsou také zavedena kritéria pro určení Českého rozhlasu, České televize a Evropského globálního navigačního družicového systému v odvětví komunikačních a informačních systému a stanic Hasičského záchranného sboru České republiky v odvětví nouzových služeb.

V průběhu roku 2015 lze tedy očekávat výrazné navýšení počtu dosud určených prvků kritické infrastruktury. V souladu s postupem stanoveným v krizovém zákoně bude „soukromé“ prvky kritické infrastruktury, jejichž provozovatelem není organizační složka státu, určovat gesční ministerstvo nebo jiný ústřední správní úřad, a to opatřením obecné povahy. Podle návrhu Ministerstva vnitra, zpracovaného na základě podkladů gesčních resortů, určí vláda svým usnesením „státní“ prvky kritické infrastruktury, tedy ty, jejichž provozovatelem je organizační složka státu.

Exkurz:
Mimořádná událost v muničním areálu Vrbětice

V dopoledních hodinách **dne 16. října 2014 došlo k požáru jednoho ze skladových objektů v areálu Vojenského technického ústavu, s.p., v obci Vlachovice-Vrbětice v okrese Zlín**. Na základě oznámení na linku 112 se na místo události dostavily složky IZS (HZS Zlínského kraje, PČR Zlínského kraje, ZZS Zlínského kraje a mobilní jednotka Krajské hygienické stanice Zlínského kraje). Velitelem zásahu složek IZS se stal, v souladu s § 19 zákona č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů (zákon o IZS), nejprve velící důstojník HZS Zlínského kraje a poté, z důvodu převažujících pyrotechnických prací na místě zásahu a střežení objektu, převzal téhož dne velení důstojník PČR.

Velitel zásahu ze zasahující jednotky HZS Zlínského kraje, pro rozsáhlost požáru a předpokládanou potřebu sil a prostředků jednotek požární ochrany (JPO), **požádal o vyhlášení nejvyššího stupně poplachu**. Z důvodu nemožnosti hasit požár, který začaly doprovázet detonace a kvůli bezprostřednímu ohrožení životů zasahujících hasičů, nařídil velitel zásahu ústup všech JPO do bezpečné vzdálenosti od hořícího objektu č. 16. Na místě bohužel zahynuli dva zaměstnanci provozovatele objektu, kteří se nacházeli v bezprostřední blízkosti místa exploze.

Přibližně za čtvrt hodiny po ústupu zasahujících jednotek došlo k obrovské detonaci a silné rázové vlně v objektu. Z důvodu míry ohrožení a rozsahu mimořádné události byl pro místo zásahu vyhlášen, v souladu s vyhláškou o IZS, zvláštní stupeň poplachu. O mimořádné události byly informovány všechny stupně velení a řízení HZS ČR a PČR. Byly svolány krizové štáby a o vzniklé situaci bylo informováno obyvatelstvo okolních obcí. Hlídky PČR uzavřely příjezdové komunikace k místu události a byla stanovena bezpečnostní zóna v okruhu téměř tří kilometrů od místa události. Na místě události nadále asistovaly JPO HZS ČR, které vybudovaly zázemí pro štáb velitele zásahu a zasahující složky. **Do řešení události se postupně zapojovaly další složky IZS**, včetně příslušníků vojenské policie. Byl povolán vojenský vrtulník k leteckému průzkumu místa události a jeho okolí, ke kterému se připojil policejní vrtulník s termovizí. Později byl k průzkumu nasazen i bezpilotní létající prostředek (dron).

Na základě rozhodnutí vlády byla dne 3. listopadu povolána Armáda České republiky (AČR). V souvislosti s řešením mimořádné události a na základě žádosti hejtmana Zlínského kraje dne 6. listopadu MV-GŘ HZS ČR zahájilo ústřední koordinaci záchranných a likvidačních prací dle § 7 odst. 3 zákona o IZS. V závislosti na postupu pyrotechnických prací v centru areálu bylo dne 22. října rozhodnuto o rozšíření preventivně bezpečnostních opatření v následujících dvou dnech.

Hlavním připraveným opatřením byla evakuace obyvatel dotčených obcí nebo jejich částí na nezbytně dlouhou dobu. **Ve dnech 23. a 24. října proběhla plánovaná evakuace v několika obcích**. Důvodem evakuace bylo umožnit pyrotechnikům průzkum několika nebezpečných míst v areálu a zabránit ohrožení z případných výbuchů. K evakuaci byly připraveny autobusy profesionálních hasičů a smluvního dopravce, sanitní vozy pro převoz imobilních občanů, evakuační centra ve Slavičíně, Vlachovicích a Valašských Kloboucích. Součástí opatření bylo také zajištění dostupnosti lékařské péče a zabezpečení stravy pro evakuované osoby.

Většina z připravených opatření nebyla nakonec realizována, protože občané využili pomoc svých rodin nebo přátel. Prostory evakuovaných částí obcí střežila PČR. Průzkumné práce pyrotechniků proběhly rychle a evakuovaní občané se mohli navrátit domů 24. října o několik hodin dříve, nežli bylo plánováno. Na úspěšném provedení evakuace měli velký podíl starostové dotčených obcí i starosta obce s rozšířenou působností Valašské Klobouky.

Dne 3. prosince došlo k výbuchu objektu č. 12. Nikdo nebyl usmrcen ani zraněn. V bezpečnostním perimetru k danému objektu jsou obce Haluzice a Lipová, z nichž musela být v důsledku této události provedena evakuace. Celkem bylo evakuováno 438 osob a kromě občanů uvedených obcí byly evakuovány Vlárské strojírny Slavičín, a.s., a Střední odborná škola Slavičín. Na základě průzkumu a celkového vývoje situace byla evakuace po dvou dnech ukončena.

Při následném pyrotechnickém průzkumu uskutečněném blíže epicentru výbuchu bylo zjištěno, že na objektu č. 11 došlo k proražení střechy plně funkčním dělostřeleckým granátem, který se zachytil ve stropním prostoru objektu. V objektu č. 11 bylo přitom uskladněno několik tisíc obdobných granátů. Ihned zasedla bezpečnostní rada Zlínského kraje, která zvážila všechna rizika, a dne 5. prosince v 18.45 hodin byla opět provedena evakuace obcí Haluzice a Lipová, jejichž obyvatelé by mohli být bezprostředně ohroženi na životě. V sobotu 6. prosince ráno byly dále evakuovány obce Vlachovice a Vrbětice, kdy bylo evakuováno přibližně 1500 osob. Pyrotechnici prováděli další průzkum místa události, a protože nenastaly žádné další nepředvídané okolnosti, evakuace byla ještě téhož dne 6. prosince ve večerních hodinách postupně ukončována v obcích Vlachovice a Vrbětice, následně pak v neděli 7. prosince ráno v obcích Haluzice a Lipová. Granát se podařilo pyrotechnikům úspěšně odstranit.

Příčiny explozí objektů č. 16 i č. 12 jsou v současné době předmětem šetření. V případě exploze prvního objektu lze uvažovat o selhání lidského faktoru při manipulaci municí. Jednou z vyšetřovacích verzí je v obou případech rovněž spáchání úmyslného trestného činu. Situace na místě zásahu je setrvalá, pod kontrolou příslušníků složek IZS. Příslušníci Pyrotechnické služby PČR provedli odklizení munice rozházené kolem dalších skladových objektů a zkontrolovali neporušenost střech objektů. V závislosti na okolnostech v místě zásahu probíhá odvoz materiálu z areálu Vrbětice do jiných skladů vlastníků a do reaktivovaných muničních skladů České republiky v Květné. **Skladové objekty v Květné budou zabezpečeny v souladu s vojenskými standardy a bude zajištěna jednak ostraha příslušníky AČR, jednak přítomnost samostatné JPO AČR**. Dosavadní průběh zásahu lze hodnotit jako plně profesionální a odpovídající požadavkům právní úpravy v oblasti IZS. Vyvážení munice bude trvat ještě minimálně jeden rok, přičemž pyrotechnická asanace areálu zabere ještě několik let.

Exkurz:
Cvičení RAFEX 2014

V termínu 27. - 29. května 2014 se v Olomouckém kraji uskutečnilo cvičení složek IZS a orgánů krizového řízení RAFEX 2014. Cílem bylo nacvičit postupy zapojení orgánů krizového řízení obce s rozšířenou působností Přerov a Olomouckého kraje do koordinace záchranných a likvidačních prací **při řešení mimořádných událostí na železnici**. Samotné cvičení mělo dvě části, a to štábní a praktickou. S ohledem na skutečnost, že do cvičení byl zapojen i modul civilní ochrany – předsunutá zdravotnická jednotka – Traumateam ČR, bylo nutné vytvořit v rámci cvičení i prostředí simulující zásah tohoto modulu v zahraničí. Z důvodu snahy procvičit co nejvíce činností jak v taktické, tak také ve strategické rovině, bylo cvičení rozděleno do několika etap, které na sebe navazovaly nebo probíhaly paralelně.

Cílem praktické části cvičení bylo nacvičit postupy složek IZS v Olomouckém kraji podle typových činností složek IZS STČ 08/IZS Dopravní nehoda, STČ 09/IZS Zásah složek IZS při mimořádné události s velkým počtem raněných a obětí a taktiku společného zásahu na železnici s jednotkami Hasičské záchranné služby SŽDC, s.o. **Námětem cvičení byla dopravní nehoda, při které se srazilo drážní vozidlo, osobní a dodávkový automobil**. Na místě nehody se nacházelo 10 zraněných osob.

Hlavní část praktického cvičení byla zaměřena na mimořádnou událost s velkým počtem zraněných na železnici. Z důvodu podemletí železniční tratě došlo k vykolejení vlaku pro přepravu osob, který následně narazil do nákladního vlaku převážejícího nebezpečnou látku – kyselinu sírovou. **Celkem zasahovalo 13 JPO**. V místě události byl zbudován štáb velitele zásahu a samotné místo zásahu bylo rozděleno na tři úseky: záchrana osob, zásah na nebezpečnou látku a dekontaminace zraněných.

Hasiči třídili zraněné metodou START, vyprošťovali osoby z převráceného vagonu a transportovali je na místo dekontaminace. Při zásahu byly využity i zkušenosti a speciální technické prostředky HZS SŽDC. Po dekontaminaci byly osoby předány místní záchranné službě, která zajistila předání zraněných Traumateamu ČR. **Nezraněným osobám byla poskytnuta psychosociální pomoc**. Do cvičení nebyla zapojena ZZS, její činnost simulovali pracovníci Fakultní nemocnice Olomouc. Celá situace byla navíc komplikována tím, že zraněné osoby nehovořily česky, ale pouze anglicky, což značně ztěžovalo komunikaci.

Cvičení RAFEX 2014 se účastnilo více než 20 subjektů, do všech částí bylo zapojeno téměř 550 osob. Cvičení potvrdilo efektivitu nastavení systému spolupráce mezi HZS Olomouckého kraje a krizovým štábem ORP Přerov a krizovým štábem Olomouckého kraje při koordinaci záchranných a likvidačních prací. Složky IZS si mohly prakticky vyzkoušet spolupráci při provádění záchranných a likvidačních prací a byly seznámeny s organizací a specifickými postupy při zásahu na železnici. Současně byly procvičeny zásady a postupy při vyslání modulu civilní ochrany - Traumateamu ČR na mezinárodní záchrannou operaci.

Exkurz:
Tragická událost ve Žďáře nad Sázavou

Dne 14. října 2014 došlo na Střední škole obchodní a služeb ve Žďáře nad Sázavou k tragické události, při níž šestadvacetiletá psychicky nemocná žena usmrtila studenta. Žena přitom podobný útok nespáchala poprvé. Již v roce 2012 napadla a pobodala vychovatelku na základní škole v Havířově-Šumbarku[2]. V den útoku ve Žďáře n. S. přišla žena do školy kolem půl osmé ráno, nejprve si obhlédla okolí, poté se vmísila mezi studenty vstupující do šaten. Jelikož je ke vstupu třeba čipové karty, prošla dovnitř v závěsu za jedním ze studentů. Žena byla ozbrojena replikou vojenského nože s čepelí dlouhou zhruba 20 cm. Školu si vybrala náhodou, jejím jediným cílem bylo spáchat útok na střední škole. Na žďárskou školu pak narazila náhodně na internetu.

Žena po příchodu do školní šatny bez varování zaútočila na sedmnáctiletou studentku, která tu seděla. Její útok směřoval na břicho. Na pomoc jí přispěchal šestnáctiletý spolužák, kterého útočnice bodla do hrudníku. Dívka, kterou se žena pokoušela vyvléci ze šatny, byla pořezána na rukou a v okamžiku boje mladíka s pachatelkou utekla. Útočnice ji chtěla dostihnout a zadržet, k čemuž použila pepřový sprej. Dívku ale nedostihla, proto si náhodně vybrala jinou oběť - další studentku, která procházela kolem. Bodla ji do břicha a odvlekla ji do jiných částí šaten, kde ji posléze držela desítky minut jako rukojmí.

Na místo zamířil policejní vyjednavač a zásahová jednotka, jež má na starosti ochranu jaderné elektrárny v Dukovanech, přítomen byl také policejní psycholog. Vyjednavač nabídl jako rukojmí sám sebe, výměnou za zadržovanou dívku, na což útočnice přistoupila. Žena po celou dobu vykřikovala, že chce na místě zásahovou jednotku, a že chce být zastřelena. A byla to právě zásahová jednotka, která ji během výměny rukojmí zadržela. K eliminaci útočnice použili policisté taser. Kromě zraněných dívek a vyjednavače byla hospitalizována také třetí dívka, která utrpěla psychický šok.

Podle později provedeného znaleckého posudku pachatelka trpí paranoidní schizofrenií, kvůli níž nemohla rozpoznat nebezpečnost jednání, ani se ovládat. Podle toxikologického posudku v době činu nebyla pod vlivem alkoholu či jiných drog.

[2] Žena v roce 2012 vtrhla do havířovské základní školy, pobodala družinářku a jako rukojmí si vzala sedmiletou dívku. Dívenku po téměř dvou hodinách vysvobodila Zásahová jednotka Krajského ředitelství policie Moravskoslezského kraje. Kvůli nepříčetnosti nebyla tehdy žena potrestána. Krajský soud v Ostravě jí počátkem roku 2013 nařídil ústavní psychiatrickou léčbu, kterou zahájila v opavské Psychiatrické nemocnici. V únoru 2014 opavský okresní soud na základě znaleckých posudků změnil ústavní léčbu na ambulantní.

Vybrané události ve sledovaném období

Červenec

XVI. ročník mezinárodní soutěže odstřelovačů na Libavé

Ve vojenském výcvikovém prostoru Libavá se sešli ti nejlepší z nejlepších odstřelovačů, aby si vyměnili zkušenosti a zároveň si porovnali své síly. Celkem sto čtyři odstřelovači soutěžili v nejrůznějších disciplínách. Odstřelovači zastupující policii byli ze zásahových jednotek Královéhradeckého, Středočeského, Ústeckého, Moravskoslezského, Jihomoravského kraje, a také zástupci cizinecké policie z Mošnova, Ruzyně a Brna - Tuřan. Nechyběli ani odstřelovači Hradní stráže.

Jednou z nejnáročnějších disciplín byla střelba na vzdálenost 675 metrů. Velmi zajímavá byla také noční střelba. Letošní počasí bylo velmi různorodé a silný déšť a vítr prověřili kvalitu závodníků. Slavnostního vyhodnocovacího večera se zúčastnili zástupci policie i armády. Vedoucí oddělení vzdělávání Policejního prezidia ČR plk. RNDr. Jiřina Hofmanová, Ph.D., poděkovala všem odstřelovačům za jejich účast v soutěži a pozvala je na další ročník. Poděkování patřilo také všem, kteří s velkým nasazením závod připravovali a také rozhodčím, kteří trpělivě závod sledovali a vyhodnocovali. Předávání cen těm nejlepším se zúčastnili také zástupci armády, mjr. Dalibor Spáčil, zástupce velitele 74. lehkého motorizovaného praporu, mjr. Milan Bielak, velitel Střediska obsluh výcvikového zařízení.

Srpen

Mimořádný počet hasičských výjezdů kvůli srpnovým bouřkám

Profesionální i dobrovolní hasiči měli plné ruce práce s odstraňováním následků bouřek, které v srpnu zasáhly naší republiku. Během večera a noci na 4. srpna 2014 vyjeli k 473 technickým pomocem (přičemž dlouhodobý denní průměr je 152 výjezdů), přičemž většinu z nich tvořily zásahy související s bouřkami. Nejvíce výjezdů zaznamenali hasiči na Vysočině, dále v Jihomoravském, Ústeckém nebo Pardubickém kraji. Oproti předcházejícím bouřkám měli naopak klidněji hasiči ve Středočeském kraji nebo v Praze. Nejčastější činností hasičů v souvislosti s přívalovými srážkami bylo odstraňování popadaných stromů a čerpání vody.

Dále hasiči odstraňovali překážky na vodních tocích, kdy čistili propusti a mosty od naplavenin, které přinesla velká voda. Dále prováděli čerpání vody ze sklepů a níže položených míst, v několika případech prováděli odčerpávání vodních lagun a také usměrňovali tok vody tak, aby nedocházelo k ohrožení majetku občanů. V Olomouckém kraji evakuovali hasiči dva dětské tábory u obce Hoštejn z důvodu zvyšující se hladiny řeky. Celkem bylo evakuováno 85 lidí, kteří byli ubytováni v obecním domě v Hoštejnu.

V Pardubickém kraji, okrese Ústí nad Orlicí, odstraňovali hasiči naplavené větve z poldru (oblast kolem vodního toku, která složí k rozlivu vody při povodních, například pole nebo louka) v Nepomukách. Dále byly preventivně strženy dvě lávky. Starostkou obce byl vyhlášen II. povodňový stupeň z důvodu zvedající se hladiny na místním toku vlivem přívalového deště. Na Vysočině v okrese Žďár nad Sázavou byl v důsledku přívalových dešťů na území obce Svratka vyhlášen III. povodňový stupeň, který byl na horním toku řeky Svratky překročen.

Dopravně bezpečnostní akce „X“

Celkem 16 913 přestupků v dopravě během necelého týdne zaznamenala Policie ČR při dopravně bezpečnostní akci s názvem „X“, která se konala od 11. srpna do 17. srpna 2014. Policisté ji vyhlásili jako reakci na nepříznivý vývoj dopravní nehodovosti v prvním pololetí roku 2014, neboť za toto období byl zaznamenán výrazný nárůst počtu dopravních nehod se smrtelnými následky. Do akce bylo nasazeno celkem 9 636 policistů, kteří zkontrolovali 93 169 vozidel, zjistili 16 913 přestupků, z toho 15 461 potrestali blokovou pokutou v celkové výši 6 300 200 Kč a 1 452 přestupků oznámili do správního řízení k dalšímu projednání.

Dopravní a pořádkoví policisté se zaměřili především na rizikové skupiny účastníků silničního provozu, kterými jsou chodci, cyklisté a řidiči motocyklů. Právě u nich je od začátku prázdnin zaznamenán nárůst tragických následků. Policisté se dále zaměřili na dodržování pravidel silničního provozu u řidičů motorových vozidel, jako je dodržování stanovené rychlosti, používání bezpečnostních pásů a zádržných systémů při přepravě dětí, telefonování za jízdy apod. V neposlední řadě hlídky pátraly po hledaných osobách, věcech a odcizených motorových vozidlech. Z celkového počtu bylo zjištěno 207 dopravních přestupků chodců, 126 dopravních přestupků cyklistů a 76 dopravních přestupků řidičů motocyklů. Řidiči se dopustili 4 731 přestupků překročení rychlosti. Celkem 358 řidičů řídilo svá vozidla pod vlivem alkoholu a 84 pak pod vlivem návykových látek. Při dopravně bezpečnostní akci hlídky odhalily 92 trestných činů (46 pod vlivem alkoholu a 7 pod vlivem návykové látky), vypátrali 14 hledaných osob a 3 odcizená vozidla.

Září

Mistrovství světa v záchranářské kynologii

Svaz záchranných brigád kynologů ČR pořádal z pověření MV-GŘ HZS ČR již 10. ročník Mistrovství ČR v záchranářské kynologii. Mistrovství České republiky se konalo v okolí obce Chbany na Žatecku. Na akci přijelo 12 kynologických týmů ze všech aktivních složek integrovaného záchranného systému České republiky, které se záchranářskou kynologií zabývají, a 1 kynologický tým ze Spolkové republiky Německo (THW Torgau).

Kynologický tým se skládal z vedoucího týmu, psovoda s atestem na sutinové vyhledávání a psovoda s atestem na plošné vyhledávání. Hlavní činností vedoucího týmu byla koordinace týmu při plnění zadaných úkolů. Prostory pro sutinové a plošné vyhledávání byly vždy vedle sebe a soutěžící prováděli činnosti současně na obou pracovištích, pro které byl stanoven i stejný časový limit. Tým byl ze základny v kempu Vikletice přepraven na pracoviště, kde probíhalo nejprve noční a poté denní nasazení celého týmu.

Základním cílem akce bylo porovnání úrovně výcviku, připravenosti a způsobu taktického nasazení kynologických týmů, to vše formou soutěžního klání. Sportovně společenská akce tohoto rozsahu také nabízí možnost uskutečnit pracovní i přátelská setkání příznivců záchranářské kynologie ze všech koutů naší země. Mistrovský titul vybojoval kynologický tým HZS ČR, který byl složen z příslušníků Záchranného útvaru HZS ČR a příslušníka HZS Pardubického kraje, na druhém místě se umístil tým Městské policie hl. m. Prahy a třetí skončil tým Policie ČR.

Nová hasičská stanice v Moravských Budějovicích

Za účasti generálního ředitele HZS ČR brig. gen. Ing. Drahoslava Ryby, starosty města Moravské Budějovice Vlastimila Bařinky, představitelů Kraje Vysočina a dalších hostů byla 5. září 2014 slavnostně otevřena stanice HZS Kraje Vysočina v Moravských Budějovicích. Výstavba stanice byla zahájena v prosinci roku 2012, s předpokládaným termínem ukončení v prosinci 2014, dokončena však byla s předstihem už v srpnu. Tento nový objekt vystavěný „na zelené louce“ nahradil stávající značně zastaralou a nevyhovující stanici v centru Moravských Budějovic u rušné hlavní silnice. Náklady na výstavbu, včetně projektové dokumentace, dosáhly částky bezmála 32 milionů korun. Budova stanice je částečně dvoupodlažní objekt s věží. Funkčně a dispozičně je stanice rozdělena na dvě samostatné a přesto propojené části, a to na požární stanici a požární zbrojnici. V objektu požární stanice byla mimo jiné vybudována tři společná garážová stání pro vozy, dílna s montážní jámou, denní místnost, zasedací místnost, pokoje, sklady a sociální zázemí. V objektu požární zbrojnice jsou například dvě společná stání pro nákladní vozy, sociální zázemí, šatny a kancelář.
Hasiči v Moravských Budějovicích vyjíždějí v průměru k téměř 200 událostem ročně. V jejich zásahové činnosti převládají technické zásahy, ale také výjezdy k dopravním nehodám, a to zejména na hlavním silničním tahu ve směru na Znojmo. Do hasebního obvodu patří mimo jiné také zámek v Jaroměřicích nad Rokytnou.

Mezinárodní policejní mistrovství zásahových jednotek

Krajské ředitelství uspořádalo Mezinárodní policejní mistrovství České republiky zásahových jednotek. Jednalo se o prestižní akci, v rámci které porovnali služební dovednosti a schopnosti policisté zařazeni u zásahových jednotek. Mistrovství se konalo pod záštitou hejtmana Moravskoslezského kraje Miroslava Nováka, přičemž Moravskoslezský kraj akci finančně podpořil poskytnutím dotace. Mistrovství se zúčastnily týmy 7 krajských policejních ředitelství, tým Útvaru rychlého nasazení, týmy ze slovenského Prešova a Žiliny a německého Sachsenu. Celkový počet 11 družstev, která se skládala z pěti policistů, kdy jeden byl vedoucím výpravy, zaručoval vysokou kvalitu soutěže.
Skladba soutěžních disciplín prověřila soutěžící po všech stránkách. Jednalo se o disciplíny nejen taktické, ale i silové a technického typu, nechyběla „záchranářská“ stanoviště. Celým mistrovstvím se pak prolínalo hledisko taktiky, volby postupu. Pro stručné přiblížení některých disciplín: zručnost a rychlost byla důležitá při disciplíně řízení vozidla. Střelecký parkúr odehrávající se na střelnici důkladně prověřil policisty jak jinak než ze střelby (mířené a časově měřené). Při lezeckém parkúru zdolávali policisté lezeckou stěnu a poté kromě jiného přemísťovali kontejner s vodou. Záchrana na vodě spočívala v několikakilometrovém běhání, překonání peřejí řeky, záchrany tonoucího a poskytnutí první pomoci. Dalšími disciplínami byl takticko-střelecký parkúr a silový víceboj.
Mistrovství Policie ČR zásahových jednotek se koná od roku 2011. Závody jsou důležité pro srovnání, ale jistě i motivačně. Policisté si rovněž vyměňují zkušenosti. Organizaci přebírá vždy příslušné krajské ředitelství, respektive jedna ze zásahových jednotek (organizátoři se tedy mistrovství z pochopitelných důvodů neúčastní). Čtvrtý ročník mistrovství lze z hlediska organizace hodnotit jednoznačně pozitivně. Organizátoři neponechali nic náhodě a precizní příprava byla vidět. Zvítězilo družstvo Útvaru rychlého nasazení, na druhém a třetím místě se umístily zásahové jednotky Krajských ředitelství policie Jihomoravského a Jihočeského kraje.

Cvičení METRO 2014

V nočních hodinách dne 22. října 2014 se uskutečnilo na území hl. m. Prahy společné taktické cvičení složek IZS a dalších subjektů krizového řízení pod názvem „METRO 2014“. Cvičení probíhalo na třech stanicích pražského metra. Další následná opatření pak navazovala ve vybraných nemocnicích v Praze. Taktické cvičení bylo realizováno na taktické, operační a strategické úrovni v souladu s typovou činností složek IZS při společném zásahu STČ 13/IZS - Reakce na chemický útok v metru.

Cílem taktického cvičení „METRO 2014“ bylo procvičit nasazení a součinnost složek IZS a dalších subjektů podílejících se na provádění záchranných a likvidačních pracích bezprostředně po uskutečněném chemickém útoku v metru. Stěžejní částí cvičení byl zásah ve stanici metra Anděl, kde došlo k teroristickému útoku rozptýlením bojové chemické látky sarin. V okamžiku příjezdu prvních JPO se ve stanici nacházelo 58 cestujících. Zásah složek IZS spočíval v koordinovaném postupu činností na místě zásahu. Mezi hlavní úkoly cvičení patřila záchrana osob a likvidace bojové chemické látky. Po dekontaminaci suchým způsobem byly zachráněné osoby předávány do péče ZZS hl. m. Prahy, která postižené dále rozvážela do nemocnic. Cvičení probíhalo současně i na sousedních stanicích metra Karlovo náměstí a Smíchovské nádraží, kde se předpokládalo další šíření bojové chemické látky.

Před čtyřmi pražskými nemocnicemi (Všeobecná fakultní nemocnice, Fakultní nemocnice Královské Vinohrady, Fakultní nemocnice Motol a Thomayerova nemocnice) byla rozvinuta stanoviště dekontaminace osob SDO 2 a SDO 3, kde byla prováděna dekontaminace cestujících, kteří opustili prostory metra před příjezdem JPO. Zde bylo dekontaminováno a ošetřeno 24 figurantů. Lékaři Ústřední vojenské nemocnice – Vojenské fakultní nemocnice Praha přijali společně s odřadem AČR 6 osob z řad složek IZS. Celkem bylo dekontaminováno a ošetřeno 78 figurantů. Dekontaminačním stanovištěm v místě zásahu prošlo 41 zasahujících. Celého cvičení se účastnilo 808 osob.

Rallye Ostrov 2014

Pod záštitou ředitele krajského policejního ředitele Ústeckého kraje plk. Mgr. Tomáše Landsfelda a ředitele zdravotnické záchranné služby Ústeckého kraje MUDr. Ilji Deyla bylo v říjnu 2014 realizováno soutěžní metodické cvičení „Rallye Ostrov 2014“, které mělo ukázat úroveň jednotnosti poskytované péče posádkami zdravotnické záchranné služby celého ústeckého kraje. Do cvičení byli vedle záchranářů a příslušníků hasičského záchranného sboru ČR také aktivně zapojeni členové lezecké skupiny zásahové jednotky Krajského ředitelství policie Ústeckého kraje.

Cvičení DUS 2014 Ostaš

Cvičení se uskutečnilo dne 15. října 2014 od 08.00 hod. ve skalním masivu Ostaš u Žďáru nad Metují, okres Náchod. V rámci cvičení bylo na Integrované operační středisko Policie ČR přijato oznámení o hrozící sebevraždě ženy. Volající oznámil, že doma našel dopis od své manželky, ve kterém uvádí, že chce asi skončit se životem. Cvičení bylo provedeno s využitím dostupných sil a prostředků zúčastněných složek IZS. Následovala pátrací akce po ohrožené osobě, její záchrana a transport těžce dostupným terénem pomocí vrtulníku LS PČR. Kromě základních složek IZS byla do cvičení dále zapojena i Skalní záchranná služba Broumovsko.

Listopad

Česká humanitární pomoc pro oblasti zasažené ebolou dorazila

2. listopadu 2014 v 18:00 vyjel nákladní automobil s doprovodným vozidlem z areálu Národní základny humanitární pomoci ve Zbirohu, aby odvezl humanitární pomoc pro oblasti západní Afriky zasažené ebolou. Zásilka v ranních hodinách dorazila do nizozemského přístavu Der Helder, kde si ji převzali zástupci nizozemského ministerstva obrany, kteří zabezpečují její dopravu do postižných zemí v západní Africe. Loď s humanitární pomocí odplula z Nizozemska dne 6. listopadu 2014. Příjemcem humanitární pomoci byla vybrána organizace „*Save the Children International*“ působící v Libérii.

Zásilka byla schválena Světovou zdravotnickou organizací a akceptována Střediskem pro koordinaci odezvy na mimořádné události Evropské komise. Humanitární pomoc převezli příslušníci Záchranného útvaru HZS ČR a styčným důstojníkem dopravy humanitární pomoci z České republiky do Nizozemí byl určen ředitel HZS Libereckého kraje plk. Ing. Roman Hlinovský, který má bohaté zkušenosti ze zahraničních misí. Hodnota poskytnuté humanitární pomoci činí 3 587 715,- Kč. Na žádost organizace Lékaři bez hranic se problémem poskytnutí humanitární pomoci zabýval Pracovní štáb Komise pro řešení výskytu závažných infekčních onemocnění v České republice a vláda České republiky. Ta svým Usnesením vlády České republiky č. 806 ze dne 1. října 2014 rozhodla, že naše země poskytne v rámci svých možností pomoc finanční a materiální. Ministerstvo zdravotnictví pro tuto humanitární akci nakoupilo 1500 ks setů ochranných pomůcek včetně filtračních polomasek a ochranných brýlí a 1600 ks dezinfekčního gelu na ruce.

Správa státních hmotných rezerv připravila pro země západní Afriky 1500 ks ochranných oděvů a 3000 ks ochranných brýlí. MV-GŘ HZS ČR vyčlenilo postiženým ze svých zásob 1500 ks ochranných oděvů, nakoupilo 1500 vaků pro transport zemřelých a zabezpečilo dopravu humanitární pomoci do Nizozemí.

Bezpečnostní akce BLUE 24

V období od 6. listopadu do 7. listopadu 2014 se uskutečnilo jedno z největších opatření pořádkové policie zaměřené na bezpečnost železnic a kontroly výkupen kovů. Do akce se zapojilo celkem 2375 policistů, kteří zkontrolovali více než 700 vlaků, téměř 1500 nádraží, 1700 sběren kovů. Zajištěno bylo 319 kg kovů, pocházejících z trestné činnosti, a také 649 g marihuany. „Mohu konstatovat, že v rámci této akce jsme zjistili tři desítky trestných činů a více než dvě stovky přestupků,“ uvedl ředitel pořádkové policie plk. Martin Hrinko.

Policisté se zaměřili na krádeže kovů, nelegální migraci a drogovou problematiku. Akce se kromě českých policistů zúčastnily i další členské státy Evropské unie. BLUE 24 byla další akcí, která napomohla v odhalení trestných činů a přestupků páchaných na železnicích. V porovnání s loňským rokem policie zajistila méně kovů, což poukazuje na zlepšení situace v krádežích na železnicích a okolí. Informace k vyhodnocení poskytl ředitel pořádkové policie plk. doc. Ing. Martin Hrinko, Ph.D., MBA a vedoucí bezpečnosti a havarijního plánování České dráhy a. s. Ing. Ota Zachariáš na dnešní tiskové konferenci.

Cvičení LETIŠTĚ 2014

Dne 5. listopadu 2014 se na Letišti České Budějovice uskutečnilo operativně taktické cvičení LETIŠTĚ 2014. Cílem cvičení bylo v praxi prověřit schopnosti jednotlivých složek Integrovaného záchranného systému reagovat v krizové situaci, v tomto případě při únosu letadla. Díky simulovanému únosu letadla, které přistálo na Letišti České Budějovice, byl spuštěn poplach TÍSEŇ, který uvedl do pohotovosti všechny složky IZS. Prakticky ukázal možnosti koordinace jednotlivých činností, byly ověřeny dojezdové časy a schopnost komunikace mezi složkami a prakticky vyzkoušeny postupy, které jsou součástí bezpečnostních plánů.

Ze strany Krajského ředitelství policie Jihočeského kraje se akce zúčastnilo 40 osob, Hasičský záchranný sbor Jihočeského kraje nasadil dvě jednotky požární ochrany České Budějovice a Křemže, které akci zajišťovaly cisternovými automobilními stříkačkami. Zapojeno bylo také hasičské operační a informační středisko. Zdravotnická záchranná služba Jihočeského kraje zde měla tým lékařů s veškerou automobilní technikou pro mimořádné situace. V neposlední řadě i Letiště České Budějovice ukázalo, že jsou na případné protiprávní jednání plně připraveni. Letoun typu L–410 s posádkou poskytlo Ministerstvo obrany České republiky z letiště Praha – Kbely. Taktické cvičení bylo následně vyhodnoceno a získané poznatky budou zařazeny do operačního plánu.

Prosinec

Přes tisíc výjezdů HZS během jediného dne – kvůli ledovce

Během pondělí 1. 12. 2014 a noci z 1. 12. na 2. 12. zaznamenaly operační střediska Hasičských záchranných sborů jednotlivých krajů zvýšený počet zásahů souvisejících s meteorologickou situací na území celé České republiky. Jednalo se především o dešťové srážky a následnou tvorbu ledovky a silné námrazy. V průběhu dne 1. 12. zasahovaly jednotky celkem u 993 technických pomocí, což je téměř sedmkrát více než je dlouhodobý denní průměr. Navýšil se i počet zásahů u dopravních nehod. K těm museli hasiči vyjet ve 191 případech, přičemž průměrně denně vyjíždějí k 50.

Pro úspěšné zvládnutí situace byly na některá krajská operační střediska povolány posily, aby mohly přijímat zvýšený počet hlášení o mimořádných událostech. Nejvíce postiženy byly kraje Vysočina, Jihomoravský, Olomoucký, Pardubický a Moravskoslezský. Jednotky profesionálních i dobrovolných hasičů vyjížděly převážně k odstraňování popadaných stromů a větví z komunikací, odstraňování spadlého elektrického vedení a vyprošťování vozidel při dopravních nehodách.

Dále hasiči zajišťovali evakuaci osob z několika vlakových souprav, které zůstaly odstavené na trati. Například v Olomouckém kraji zůstaly stát vlaky plné cestujících (celkem asi 300 osob). Vzhledem k fungujícím trolejím měli cestující zajištěno celou noc teplo a světlo. Ve stanicích Drahotuše a Lipník nad Bečvou byly přistaveny rychlíky s jídelními vozy, kde měli cestující možnost si zakoupit občerstvení. Přepravce jim také zabezpečil vodu a v ranních hodinách všechny železniční stanice objížděli hasiči, kteří čekajícím cestujícím rozdávali vodu a lehké občerstvení. V okrese Kroměříž bylo evakuováno 37 osob z vlaku uvízlého na trati z důvodu výpadku elektrického trakčního vedení, osoby byly přepraveny autobusem HZS Zlínského kraje na nádraží Přerov.

Dálniční policisté mají sedm nových speciálů

Vedení policejního prezidia dnes v poledne převzalo sedm nových služebních vozidel ŠKODA Superb 3,6 FSI V6 4x4. Nové dálniční speciály v civilním provedení pořídila Policie ČR v rámci obměny stávajícího vozového parku určeného k výkonu služby speciálně na dálničních odděleních. Nahradí tak některá z vozidel VW Passat R36. Nové vozy z rukou zástupců společnosti ŠKODA AUTO převzal náměstek policejního prezidenta pro ekonomiku plk. Ing. Petr Petřík. Slavnostního předání se v Zákaznickém centru v Mladé Boleslavi zúčastnil i ředitel ředitelství služby dopravní policie Policejního prezidia ČR plk. Ing. Tomáš Lerch.

Nová policejní vozidla se zrychlením z 0 – 100 km/h za 6,4 sekundy a maximální rychlostí 250 km/h tak budou sloužit policistům v Rudné u Prahy, Nové Vsi, Poříčanech, Ostrově u Stříbra, Velkém Beranově, Ivanovicích na Hané a Podivíně. Po vozidlech typu Volkswagen Passat R36 a B7 jsou tak vozidla ŠKODA Superb dalším nástrojem pro odhalování a postihování toho nejnebezpečnějšího chování řidičů, se kterým se v dálniční síti setkáváme. Výhodou pro plnění úkolů skrytého dohledu na bezpečnost silničního provozu je, že automobily tohoto typu jsou na českých silnicích k vidění poměrně často.

Zdroje pro tuto kapitolu: MV-GŘ HZS ČR, PČR, telegraph.co.uk, zzshmp.cz, sshr.cz, eagri.cz, pozary.cz, cez.cz, ceps.cz

NOVINKY V LEGISLATIVĚ ČR ZA SLEDOVANÉ OBDOBÍ

Energetika a energetická bezpečnost

87/2014 Sb., **kterým se mění zákon č. 201/2012 Sb., o ochraně ovzduší**
http://portal.gov.cz/app/zakony/zakonPar.jsp?page=0&idBiblio=82074&recShow=0&name=~2F2014&rpp=100#parCnt

90/2014 Sb., **kterým se mění zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon), ve znění pozdějších předpisů, a zákon č. 165/2012 Sb., o podporovaných zdrojích energie a o změně některých zákonů, ve znění pozdějších předpisů**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=82077&name=~2F2014&rpp=100#local-content

111/2014 Sb., **o celkovém množství elektřiny a plynu spotřebovaném v České republice v roce 2013**
http://portal.gov.cz/app/zakony/zakonPar.jsp?page=0&idBiblio=82221&name=~2F2014&rpp=100#local-content

193/2014 Sb., **o způsobech a termínech účtování a hrazení ceny na úhradu nákladů spojených s podporou elektřiny a o provedení některých dalších ustanovení zákona o podporovaných zdrojích energie**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=82553&name=~2F2014&rpp=100#local-content

195/2014 Sb., **o způsobu regulace cen a postupech pro regulaci cen v plynárenství**
http://portal.gov.cz/app/zakony/zakonPar.jsp?page=0&idBiblio=82582&name=~2F2014&rpp=100#local-content

Bezpečnost finančních institucí

31/2014 Sb., **kterou se mění vyhláška č. 141/2011 Sb., o výkonu činnosti platebních institucí, institucí elektronických peněz, poskytovatelů platebních služeb malého rozsahu a vydavatelů elektronických peněz malého rozsahu**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=81737&name=~2F2014&rpp=100#local-content

163/2014 Sb., **o výkonu činnosti bank, spořitelních a úvěrových družstev a obchodníků s cennými papíry**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=82460&src=nove&rpp=15#local-content

216/2014 Sb., **kterou se mění vyhláška č. 346/2013 Sb., o předkládání výkazů bankami a pobočkami zahraničních bank České národní bance**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=82716&name=~2F2014&rpp=100#local-content

Informační kriminalita a kybernetická bezpečnost

181/2014 Sb., **o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=82522&name=~2F2014&rpp=100#local-content

258/2014 Sb., **kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a zákon č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=82911&name=~2F2014&rpp=100#local-content

315/2014 Sb., **kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=83169&name=~2F2014&rpp=100#local-content

316/2014 Sb., **o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=83170&name=~2F2014&rpp=100#local-content

317/2014 Sb., **o významných informačních systémech a jejich určujících kritériích**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=83171&name=~2F2014&rpp=100#local-content

Krizové řízení

69/2014 Sb., **o technických podmínkách věcných prostředků požární ochrany**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=81926&name=~2F2014&rpp=100#local-content

123/2014 Sb., **o bezpečnostních a technických požadavcích na zacházení s pyrotechnickými výrobky**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=82301&name=~2F2014&rpp=100#local-content

221/2014 Sb., **kterou se mění vyhláška č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci)**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=82748&name=~2F2014&rpp=100#local-content

259/2014 Sb., **o prekurzorech výbušnin a o změně zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=82912&name=~2F2014&rpp=100#local-content

315/2014 Sb., **kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=83169&name=~2F2014&rpp=100#local-content

KONFERENCE A SETKÁNÍ

Připravované akce v ČR a v SR v roce 2015

Energetika a energetická bezpečnost

19. – 22. 1. 2015 **Infotherma 2015**
22. ročník mezinárodní výstavy k vytápění, úsporám energií a smysluplnému využívání obnovitelných zdrojů
Výstaviště Černá Louka, Ostrava
http://www.infotherma.cz/cs/

22. – 24. 1. 2015 **Solar Praha 2015**
Veletrh zaměřený na úspory energií a alternativní zdroje energie
Praha, PVA Letňany
www.pva.cz/cz/kalend.asp?id=8597

22. – 24. 1. 2015 **Solar Praha 2015**
Veletrh zaměřený na úspory energií a alternativní zdroje energie
Praha, PVA Letňany
www.pva.cz/cz/kalend.asp?id=8597

25. – 28. 3. 2015 **Racioenergia**
25. mezinárodní veletrh využití energie
Bratislava - Incheba, Slovensko
www.incheba.sk

25. – 28. 3. 2015 **Obnovitelné zdroje energie**
Nitra - Agrokomplex, Slovensko
www.agrokomplex.sk

2. 4. 2015 **Pražské evropské energetické fórum 2015**
25. mezinárodní veletrh využití energie
Praha, Lichtenštejnský palác
http://www.energyforum.cz/

21. – 23. 4. 2015 **Dny teplárenství a energetiky 2015**
Kongresové centrum ALDIS, Hradec Králové
www.dnytepen.cz

6. – 7. 10. 2015 **ElfetexFest Plzeň**
21. ročník veletrhu elektrotechniky, elektroniky a energetiky
Parkhotel Plzeň, Plzeň
http://www.omnis.cz

18. – 20. 11. 2015 **FOR ENERGO**
3. mezinárodní veletrh výroby a rozvodu elektrické energie
PVA EXPO PRAHA, Praha
www.forenergo.cz

Bezpečnost finančních institucí

22. 9. 2015 **Security 2015**
IT bezpečnost včetně internetového bankovnictví
Clarion Congress Hotel Prague
http://www.aec.cz/cz/konference

22. 9. 2015 **Data Storage Workshop**
9. ročník konference o zálohování, ukládání, archivaci a správě dat
Konferenční centrum City, Praha
http://www.dsw.cz/

6. 10. 2015 **Svět informatiky ve finančnictví**
Konference o novinkách v oblasti moderního bankovnictví a bezpečnosti
Konferenční centrum City, Praha
http://financnictvi.konference.cz/

Informační technologie a kyberbezpečnost

24. 3. 2015 **IT Security Workshop**
Rozmach kybernetického zločinu vs. zajištění a udržení bezpečnosti v oblasti IT. Kybernetický zákon. Security Management. Ochrana zařízení, programů a dat. Bezpečnost a monitoring sítí. DDoS útoky. Mobile Device Management.
Konferenční centrum City, Praha
http://www.itsw.cz/

16. 4. 2015 **Advanced Threat Protection Network Security Conference**
IDC Cema, Praha
http://www.ictsecurity.cz/details/696.html

9. 6. 2015 **Cloud Computing Conference**
Konference o cloud computingu, moderní ochraně dat a bezpečnosti
Hotel Crowne Plaza, Bratislava
http://ccc.exponet.sk/

16. 6. 2015 **Sociální sítě a bezpečnost**
AFCEA, význam sociálních sítí a možnosti jejich zneužití
Praha
http://www.ictsecurity.cz/details/700.html

22. 9. 2015 **Security 2015**
IT bezpečnost včetně internetového bankovnictví
Clarion Congress Hotel Prague
http://www.aec.cz/cz/konference

22. 9. 2015 **Data Storage Workshop**
9. ročník konference o zálohování, ukládání, archivaci a správě dat
Konferenční centrum City, Praha
http://www.dsw.cz/

1. 10. 2015 **Cyber Security 2015**
Odborná konference kybernetické bezpečnosti
Praha, místo bude upřesněno
http://www.idg.cz

20. 10. 2015 **Bezpečnosť a dostupnosť dát**
Komplexná ochrana informačných systémov
Hotel Crowne Plaza, Bratislava
http://bdd.exponet.sk/

Krizové řízení

24. – 25. 3. 2015 **Konference Červený kohout**
18. ročník konference s mezinárodní účastí
Wellness Hotel Frymburk
http://www.cervenykohout.com/

19. - 21. 5. 2015 **PYROS/ISET**
Mezinárodní veletrh požární a bezpečnostní techniky a služeb
Brno, Výstaviště
www.bvv.cz/pyros-iset

19. - 21. 5. 2015 **Interprotec**
Mezinárodní veletrh prostředků osobní ochrany, bezpečnosti práce a pracovního prostředí
Brno, Výstaviště
www.bvv.cz/interprotec

28. – 30. 5. 2015 **XXI. Mezinárodní konference o separační chemii a analýze toxických látek**
Institut ochrany obyvatelstva, Lázně Bohdaneč
http://www.hzscr.cz/clanek/institut-ochrany-obyvatelstva-menu-informacni-servis-zpravodajstvi-xxi-mezinarodni-konference-o-separacni-chemii-a-analyze-toxickych-latek.aspx

1. – 3. 6. 2015 **Fireco 2015**
12. mezinárodní veletrh požární, záchranářské a zabezpečovací techniky
Trenčín, Slovensko
http://www.expocenter.sk

15. - 19. 9. 2015 **FSDAYS 2015, Prague Fire & Security Days**
7. mezinárodní veletrh nejnovějších trendů v oboru požární a zabezpečovací techniky, systémů a služeb
Praha, PVA Letňany
www.fsdays.cz

Připravované akce v zahraničí

Energetika a energetická bezpečnost

23. – 27. 3. 2013 **FIEE 2015**
28. mezinárodní veletrh energetiky a elektroniky
Sao Paulo, Brazílie
http://www.fiee.com.br/en/

15. – 17. 4. 2015 **ISC West 2015, International Security Conference West**
Bezpečnost staveb, požární ochrana a nové technologie v průmyslu
Las Vegas, Nevada, USA
http://www.iscwest.com

8. – 10. 7. 2015 **Office Disaster Prevention Expo**
Mezinárodní výstava specializující se na krizové řízení a havarijní plánování
Tokio, Japonsko
http://www.reedexpo.com

28. – 30. 6. 2016 **World Nuclear Exhibition 2016**
Mezinárodní veletrh jaderné energie
Paříž, Francie
http://www.world-nuclear-exhibition.com/

8. – 11. 11. 2016 **Electronica 2016**
Mezinárodní veletrh elektronických komponent, doplňků a materiálů
Mnichov, Německo
http://www.electronica.de/

Bankovnictví a finanční bezpečnost

6. – 8. 10. 2015 **IT-SA**
Mezinárodní veletrh pro IT bezpečnost a ochranu, včetně online bankingu
Norimberk, Německo
http://www.it-sa.de/

17. – 19. 11. 2015 **Cartes 2015**
Světový veletrh digitálního zabezpečení, karet a identifikací
Paříž, Francie
http://www.cartes.com/

Informační technologie a kyberbezpečnost

2. – 4. 6. 2015 **Infosecurity Europe**
Výstava zabezpečení informací, informačních technologií a zdrojů
Londýn, Anglie
http://www.infosecurityeurope.com

15. – 17. 7. 2015 **Security 2015**
Výstava technologií zabezpečení, bezpečnosti IT, služeb a systémů
Melbourne, Austrálie
http://www.securityexpo.com.au

1. - 6. 8. 2015 **Black Hat USA 2015**
Konference o kybernetické bezpečnosti a fenoménu hackingu
Mandalay Bay, Las Vegas, USA
https://www.blackhat.com/us-15/

24. 8. 2015 **IWCF 2015**
International Workshop on Computational Forensics
Stockholm, Švédsko
http://www.allconferences.com/c/international-workshop-on-computational-forensics-stockholm-2014-august-24

23. – 25. 9. 2015 **Infosecurity Russia**
Výstava zabezpečení informací, informačních technologií a zdrojů
Moskva, Rusko
http://www.reedexpo.com

10. – 13. 11. 2015 **Black Hat Europe 2015**
Konference o kybernetické bezpečnosti a fenoménu hackingu
Amsterdam, Nizozemsko
https://www.blackhat.com/

Krizové řízení

18. – 20. 1. 2015 **Intersec 2015**
Mezinárodní výstava bezpečnosti a bezpečnostní techniky
Dubaj, Spojené arabské emiráty
http://www.intersecexpo.com

10. – 12. 2. 2015 **Security & Safety Technologies**
20. mezinárodní výstava bezpečnostní techniky
Moskva, Rusko
http://www.security-moscow.com

3. – 5. 3. 2015 **Global Security Asia**
Mezinárodní výstava vnitrostátní bezpečnostní techniky
Singapur
http://www.globalsecasia.com

10. – 12. 3. 2015 **ISC Brazil**
Největší latinskoamerický veletrh bezpečnostního průmyslu
Sao Paulo, Brazílie
http://www.reedexpo.com

24. – 26. 3. 2015 **DIHAD**
Mezinárodní výstava prostředků pro humanitární pomoc
Dubaj, Spojené arabské emiráty
http://www.dihad.org

25. – 26. 3. 2015 **Infosecurity BE & Storage Expo Belgium**
Výstava bezpečnostní techniky
Brusel, Belgie
http://www.reedexpo.com

25. – 26. 3. 2015 **Security Expo**
Mezinárodní specializovaná výstava – bezpečnost a ochrana
Sofie, Bulharsko
http://www.iec.bg

13. – 16. 4. 2015 **MIPS**
Mezinárodní výstava bezpečnosti a požární ochrany
Moskva, Rusko
http://www.mips.ru

15. – 17. 4. 2015 **ISC West 2015, International Security Conference West**
Bezpečnost staveb, požární ochrana a nové technologie v průmyslu
Las Vegas, Nevada, USA
http://www.iscwest.com

21. – 22. 4. 2015 **Border Security Expo**
Výstava bezpečnosti a ochrany hranic
Phoenix, Arizona, USA
http://www.bordersecurityexpo.com

21. – 22. 4. 2015 **Counter Terror Expo**
Mezinárodní výstava a konference k boji proti terorismu
Londýn, Velká Británie
http://www.counterterrorexpo.com

28. – 31. 5. 2015 **International Hazardous Material Response Teams Conference**
Konference a výstava týkající se nebezpečných látek, zbraní hromadného ničení, terorismu, bioterorismu atd. Výstavní plocha zahrnuje venkovní ukázky nebezpečných látek, zařízení a vybavení.
Baltimore, Maryland, USA
http://www.iafc.org

8. – 13. 6. 2015 **Interschutz**
Přední světový veletrh zaměřený na požární ochranu, záchranářství, zmírňování následků katastrof, bezpečnost a ochranu.
Hannover, Německo
http://www.interschutz.de

8. – 10. 7. 2015 **Office Disaster Prevention Expo**
Mezinárodní výstava specializující se na krizové řízení a havarijní plánování
Tokio, Japonsko
http://www.reedexpo.com

26. – 29. 8. 2015 **Fire-Rescue International 2015**
Konference a mezinárodní veletrh k problematice požární ochrany, zdravotnického záchranářství a odborného vzdělávání
Atlanta, Georgia, USA
http://www.iafc.org

22. – 24. 9. 2015 **Firetech 2015; Arms and Security 2015**
IX. mezinárodní specializovaná výstava protipožárních technologií; XII. mezinárodní výstava vojenské a policejní techniky
Kyjev, Ukrajina
http://www.iec-expo.com.ua

5. – 7. 10. 2015 **Fire India**
Největší veletrh zaměřený na požární ochranu a bezpečnost průmyslu v asijsko-pacifickém regionu
Nové Dillí, Indie
http://www.reedexpo.com

17. – 20. 11. 2015 **Milipol 2015**
Mezinárodní výstava vnitřní bezpečnosti státu
Paříž, Francie
http://www.milipol.com

Zdroje použité pro monitoring

MV, PČR, HZS ČR, MPO, MO, MZV, ČTK, vlada.cz, idnes.cz, ceps.cz, cez.cz, mero.cz, pressweb.cz, energetickakoncepce.cz, prumysl.cz, ČT 24, ČRo, net4gas.cz, cepsr.com, banktech.com, lidovky.cz, tpeb.cz, euraktiv.cz, eagri.cz, europa.eu, ihned.cz, eset.cz, root.cz, computerworld.cz, itbiz.cz, mcaffee.com, amazongenius.com, krebsonsecurity.com, zachranny-kruh.cz, mayerbrown.com, isis-europe.eu, population-protection.eu, cad.cz, skpz.cz, bivs.cz, konference.org, novinky.cz, itsw.cz, isss.cz, forum2000.cz, bvv.cz, spi.unob.cz, cabm.cz, sdiwc.net, asisonline.org, counterterrorexpo.com, expopromoter.com, waset.org, iaem.com, it-trans.org, aem.cz, konference.ncbi.cz, ictsecurity.cz, khkjm.cz, muptimes.cz, ohk-most.cz, securiteknews.wordpress.com, cy2012.eu, eur-lex.europa.eu, csas.cz, denik.cz, csob.cz, root.cz, labs.nic.cz, govcert.cz, cesnet.cz, saferinternet.cz, bbc.com, bezpecnyinternet.cz, ceskenoviny.cz, zpravy.tiscali.cz, zdnet.com, net-security.org, radyvnouzi.cz, portal.gov.cz, konferenceit.cz, security-portal.cz, itnetwork.cz, tyinternety.cz, cbss.cz, iir.cz, sbp.fsv.cuni.cz, vojenskaskola.cz, dspace.k.utb.cz, mup.cz, veletrhyavystavy.cz, blackhat.com, banksecurityportal.com, business-continuity.com, pro-energy.cz, energetika.cz, euroexpo.cz, europeum.org, cleverandsmart.cz, technet.idnes.cz, aktualne.centrum.cz, ceskatelevize.cz, enviweb.cz, tretiruka.cz, cyprus-mail.com, prumysl.cz, europol.europa.eu, aphaia.co.uk, allpremium4.blogspot.com, zive.cz, e15.cz, trustport.com, telegraph.co.uk, zzshmp.cz, kickstarter.com, interpol.int, hpsolutions.cz, bakerstreet.wikia.com, cnb.cz, newmoney.gov, ppas.cz, pozary.cz, economist.com, csoonline.com, edition.cnn.com, enisa.europa.eu, en.wikipedia.org, tomshardware.com, stanford.edu, chip.cz, newscientist.com, russelwebster.com, businessworld.cz, infoworld.com, europa.eu, itnewsafrica.com, scmagazine.com.au, businessinsider.com, rozhlas.cz, reko a.s., atominfo.cz, bihdaytonproject.com, eon.cz, elektrika.cz, spiegel.de, thermoil.cz, investicniweb.cz, ceskapozice.lidovky.cz, patria.cz, openiazoch.zoznam.sk, energetika.tzb-info.cz, cbap.cz, barchart.com, policie.cz, brnensky.denik.cz, policejnidenik.cz, btctip.cz, cnews.cz, bankovnipoplatky.com, gstylemag.com, diit.cz, echo24.cz, m-journal.cz, danielzstinson.wordpress.com, pcworld.com, symantec.com, ec.europa.eu, csze.cz, power-engineering.sk, svetsiti.cz, ictsecurity.cz, aec.cz, biom.cz, konferenceit.cz, expo-net.cz, eventworld.cz, cebit.de, allconferences.com, blackhat.com, veletrhyavystavy.cz, fsdays.cz

Zdroje obrázky

obrázky byly čerpány z výše uvedených zdrojů + ze zdrojů:

sxc.hu, ceps.cz, bloglobal.net, cez.cz, itbiz.cz, ceskatelevize.cz, temelinky.cz,

Text neprošel jazykovou a stylistickou úpravou.