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. ledna do 30. června 2014

Odbor bezpečnostní politiky Ministerstva vnitra

srpen 2014

OBSAH

ÚVODEM

Vážení čtenáři,

dostává se Vám do rukou periodická situační zpráva, která mapuje vybrané oblasti bezpečnosti v první polovině roku 2014. 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, působících 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 bezpečnosti finančních institucí je tak zvláštní oddíl věnován rizikům, spojeným s novým fenoménem virtuálních platidel.

V sekci o kybernetické bezpečnosti a informační kriminalitě čtenář nalezne oddíl zvlášť věnovaný novému zákonu o kybernetické bezpečnosti, kapitola zaměřená na energetickou bezpečnost pro změnu obsahuje exkurz o útocích na kritickou infrastrukturu. Kapitola o krizovém řízení je rozšířena o přehled připravovaných velkých cvičení v roce 2014 a 2015.

Poslední dvě kapitoly 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 konference a setkání, 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 kapitolu, 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 prvním pololetí roku 2014. Z policejních statistik se zde dozvídáme pozitivní zprávu o významném poklesu počtu zjištěných trestných činů, kdy celková kriminalita byla vůbec nejnižší za posledních 10 let. Finanční instituce, jejichž bezpečnost patří mezi hlavní zájmové okruhy této situační zprávy, jistě potěší téměř třetinový pokles počtu loupežných přepadení bank a spořitelen. K nárůstu bohužel stále dochází u drogové kriminality, a to zejména v česko-německém pohraničí.

Konkrétnější data je možné nalézt v následujících kapitolách věnovaných jednotlivým oblastem bezpečnosti. Kapitola o energetické bezpečnosti nabízí bližší pohled na hlavní trendy v české a evropské energetice, delší exkurz je pak věnován cíleným útokům na kritickou infrastrukturu, ke kterým naštěstí dochází v České republice velmi zřídka. Největší problémy tak způsobují především krádeže a podvody různého rozsahu. Vedle nich jsou to samozřejmě také nehody a mimořádné události, o kterých pojednávají statistiky Hasičského záchranného sboru. Mezi ty největší patřil dubnový požár rozvodny velmi vysokého napětí v pražském Slivenci, se škodou převyšující 8 milionů korun Kč. Zvláštní oddíl je věnován cvičením BLACKOUT a SAFEGUARD DUKOVANY.

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. Internacionalizaci organizovaných balkánských skupin, věnujících se skimmingu a zneužívání kreditních karet, dokládají popsané případy mezinárodní policejní spolupráce za asistence Europolu. Na to, že moderní fenomén virtuálních platidel má i řadu rizik a úskalí, upozorňuje delší exkurz v závěru kapitoly. Velkou hrozbu v tomto směru představuje zneužívání virtuálních měn k organizovanému zločinu (např. obchodu s drogami), praní špinavých peněz a financování terorismu.

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 nemalý nárůst trestné činnosti páchané s pomocí výpočetní techniky. Kromě tradiční sekce věnované aktivitám bezpečnostních složek a státní správy při boji s tímto fenoménem je delší exkurz věnován připravovanému zákonu o kybernetické bezpečnosti, který v současné době prochází legislativním procesem. Česká republika se jeho přijetím stane jednou z prvních evropských zemí, které mají problematiku kybernetické bezpečnosti upravenu zvláštním zákonem. Kapitola také obsahuje přehled nových hrozeb, jakými byl ve sledovaném období např. nový malware napadající routery, či fenomén Heartbleed bug.

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 první poloviny roku a velkých cvičení, která jsou v budoucnu plánována. Zvláštní exkurzy blíže popisují např. cvičení Nákaza 2014.

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 30. 6. 2014 Policie ČR registrovala celkem 154 172 trestných činů (-13 354, -8 %). Nárůst zaznamenaný v roce 2013 byl eliminován a celková kriminalita za 1. pololetí roku 2014 byla naopak nejnižší za posledních 10 let.

Zjištěná kriminalita celkem meziročně poklesla o 8 %.

Počet objasněných trestných činů se snížil o 0,4 %.

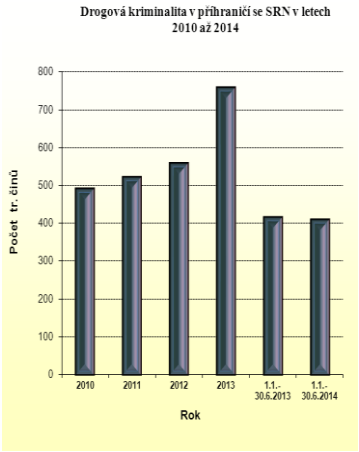
K poklesu došlo u násilné i majetkové kriminality. Meziročně naopak vzrostla kriminalita mravnostní a hospodářská:

- násilná kriminalita (-6,5 %)
- mravnostní kriminalita (+1,6 %)
- majetková kriminalita (-12,9 %)
- ostatní kriminalita (-2,6 %)
- zbývající kriminalita (+6,3 %)
- hospodářská kriminalita (+1,8 %)

Zjištěné škody poklesly o 1,3 %, zajištěné hodnoty poklesly o cca 29,3 %.

Objasněno bylo 60 700 skutků (-266, -0,4 %). Pokles zjištěné kriminality tak jako obvykle provází i pokles počtu objasněných trestných činů. **Celková objasněnost naopak meziročně vzrostla z 36,4 % na 39,4 %, a byla tak nejvyšší za posledních 10 let.**

Aktuální prioritou ministra vnitra a PČR je boj proti drogové kriminalitě, zvláště v příhraniční se SRN. Její negativní vývoj od roku 2010 ukazuje následující graf.



[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.

Vybrané markanty registrované kriminality

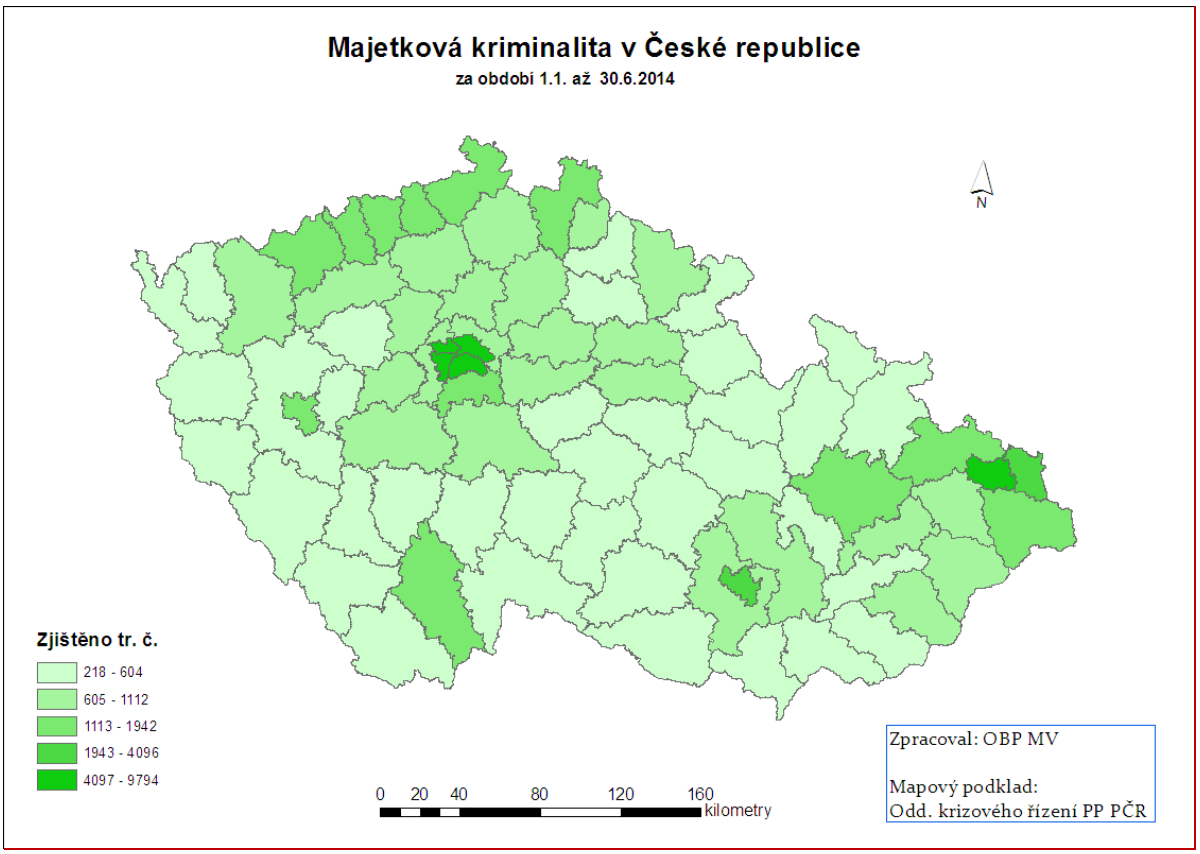
Zjištěné hmotné škody meziročně **poklesly** o 1,3 % na cca **15,8 mld. Kč**

V rámci násilné kriminality významně poklesl např. počet loupeží (-16,7 %), **loupeže na finančních institucích poklesly o 30,3 %**.

Počet majetkových trestných činů se meziročně snížil o 13 710, tj. 12,9 %, snížily se počty všech druhů krádeží vloupáním, z toho do obchodů o 29,6 %, do rodinných domků o 18,2 %. V rámci krádeží prostých poklesly krádeže kapesní (-25,8 %) a také krádeže věcí z aut (-20,4 %).

Dlouhodobý nárůst – a to nejen v příhraničí se SRN – naopak vykazuje drogová kriminalita, i když jeho dynamika se v posledním pololetí poněkud snížila. Např. počet zjištěných trestných činů nedovolená výroba a jiné nakládání s omamnými a psychotropními látkami a s jedy (§ 283 TZ) celostátně meziročně vzrostl o 7 %.

Významný meziroční nárůst se projevil také např. u trestného činu znásilnění (+21 %) – v rámci mravnostní kriminality, krádeže jízdních kol (+11 %) – v rámci majetkové kriminality, úvěrový podvod (+10,2 %) – v rámci hospodářské kriminality.



Stíhané a vyšetřované osoby

V 1. pololetí roku 2014 bylo celkem **stíháno a vyšetřováno 59 523 osob**. Meziroční vývoj je patrný z tabulky 1. Je zřejmé, že došlo k mírnému poklesu počtu stíhaných a vyšetřovaných osob (-430, -0,7 %), což koresponduje s nižším počtem objasněných trestných činů.

Recidivisté soustavně „posilují“ a jejich podíl na celkovém počtu stíhaných a vyšetřovaných osob dosáhl ve sledovaném období již **53,8 %.** Enormní dlouhodobý nárůst tohoto podílu dokumentují následující data za celé roky: 52,6 % v roce 2013, 50 % v roce 2012, pouze **29,7 % v roce 2000**. Stále tedy platí, že postupy aplikované v ČR k eliminaci recidivy trestné činnosti jsou bohužel neúčinné.

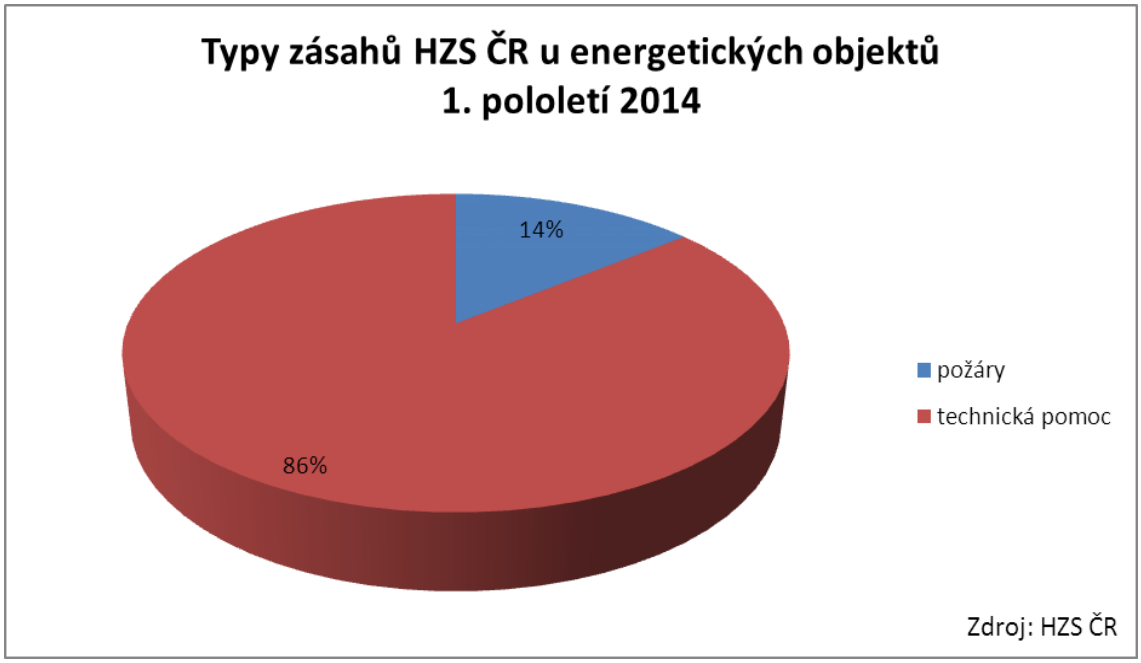
	2013	tj. %	2014	tj. %
Celkem osob	59 953	100,0	59 523	100,0
recidivisté	**31 275**	**52,2**	**32 023**	**53,8**
nezletilí do 15 let	639	1,1	673	1,1
mladiství 15 až 18 let	1 509	2,5	1 365	2,3
ženy	8 411	14,0	8 663	14,6
cizinci	3 818	6,4	3 675	6,2

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

ENERGETICKÁ BEZPEČNOST

Hasičské statistiky a jejich interpretace

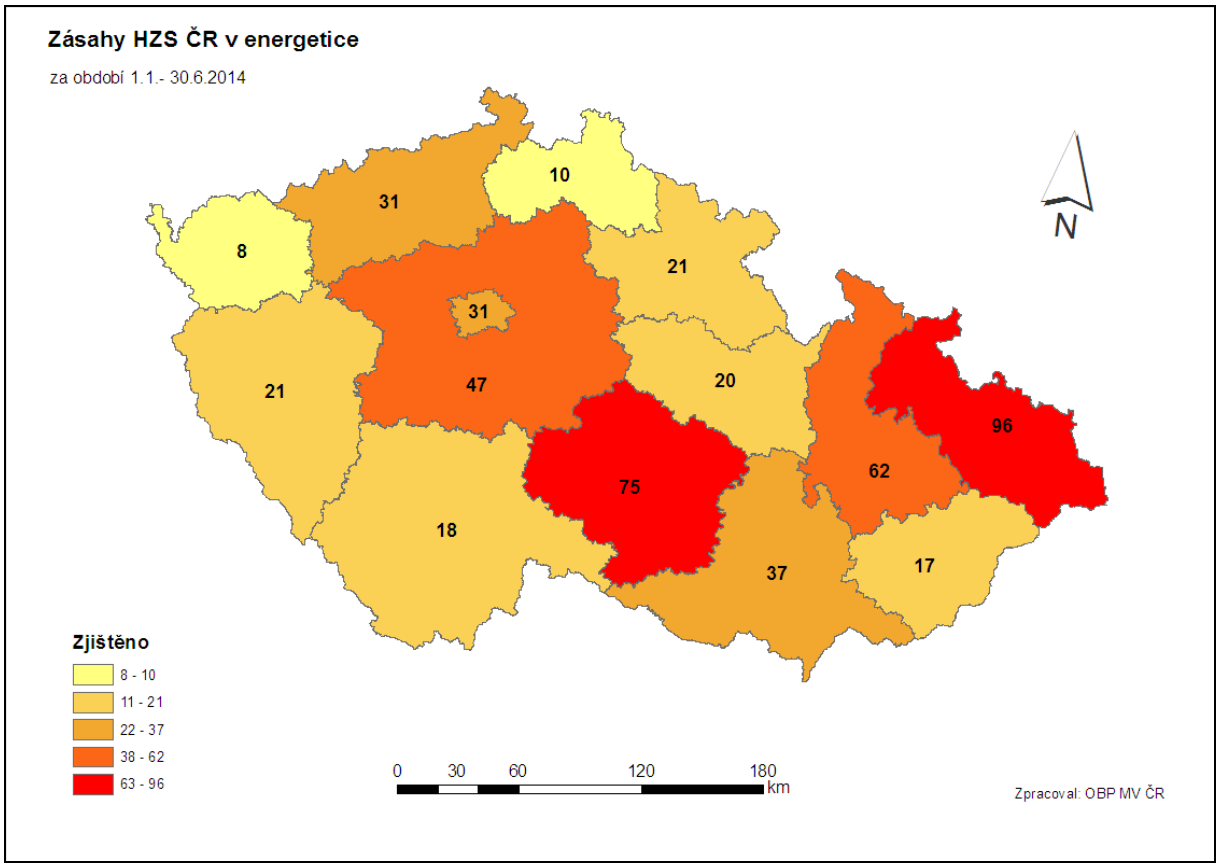
První polovina roku 2014 byla z hlediska mimořádných událostí v energetické infrastruktuře o něco málo příznivější než 2. pololetí roku 2013. Jednotky Hasičského záchranného sboru zasahovaly v **celkem 494 případech u objektů souvisejících s energetikou**. Z toho jen 70 výjezdů se přímo týkalo požárů. Celých 86 % případů spadá do rozsáhlé kategorie technická pomoc.



Pod technickou pomocí se skrývají 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, padající sloupy elektrického vedení, úniky páry atd.

Na rozdíl od předchozího pololetí nebyl ani v jednom případě vyhlášen tzv. II. stupeň poplachu, což znamená, že nebylo nutné zapojit velké množství hasičských jednotek. Žádná z řešených událostí tedy nepřerostla v havárii většího rozsahu.

Z níže přiložené mapy vyplývá, že v důsledku mimořádných událostí nejvíce trpí energetická infrastruktura v Moravskoslezském kraji. Tento kraj vede v tomto ohledu již řadu let – jedním z možných vysvětlení je velké množství zde přítomných energetických a těžebních provozů. Překvapivě vysoký počet zásahů opět zaznamenal také kraj Vysočina. Ten se tradičně potýká zejména s poškozením elektrické sítě v důsledku větru a mrazů. Na třetím místě skončil kraj Ústecký. Naopak nejméně mimořádných událostí bylo v tomto odvětví zaznamenáno v kraji Karlovarském (pouhých 8). Je přitom zajímavé, že ve čtyřech z těchto osmi případů se jednalo o pád či poškození sloupu veřejného osvětlení.



Připomeňme, že v průběhu roku 2013 hořelo v energetických budovách celkem v 98 případech (což je 15% nárůst oproti roku 2012) a škoda přesáhla 187 milionů korun. Hasičům se nicméně podařilo uchránit hodnoty v celkovém objemu více než 250 milionů korun. O život při těchto požárech přišel jeden člověk a šest lidí bylo zraněno.

V prvním pololetí roku 2014 hořelo celkem 70x v objektech výroby a rozvodu elektřiny a plynu. Celková škoda převyšovala 22 milionů korun a zraněny byly 4 osoby. Na závěr tradičně přehled velkých požárů první poloviny roku 2014 s dopadem na energetickou infrastrukturu:

Největší požáry související s energetikou v 1. pololetí roku 2014

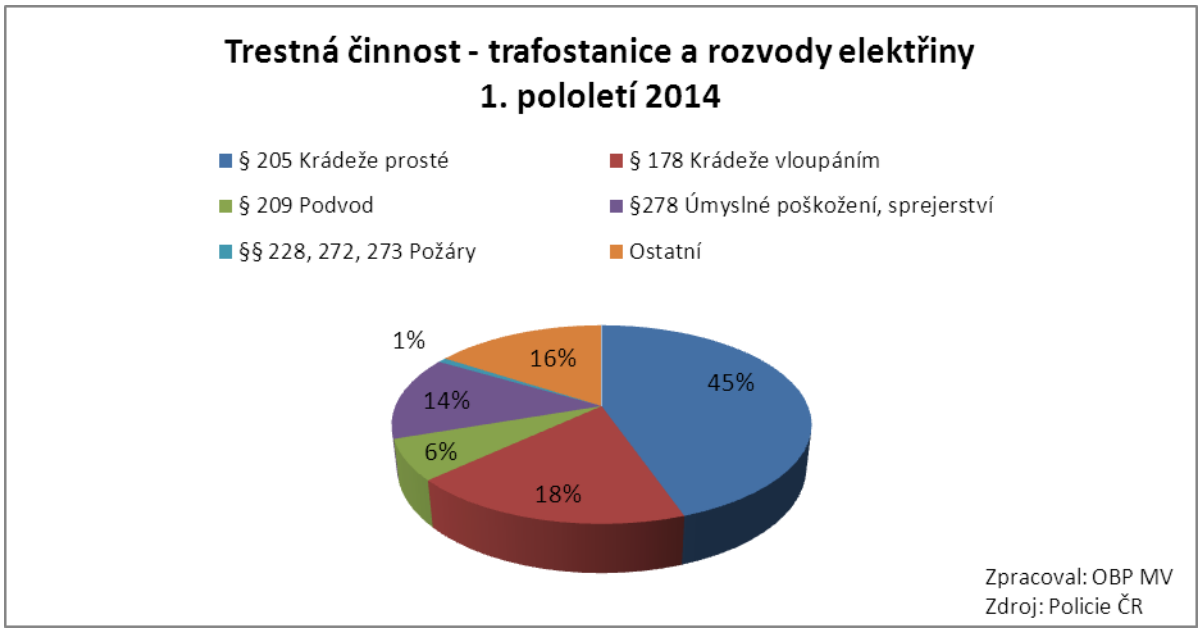
28. 6. – **Rozvodna fotovoltaické elektrárny**, Valašské Příkazy, okr. Vsetín.
Příčina – v šetření.
Škoda – 4 000 000 Kč, požár likvidovalo 5 jednotek PO.

14. 6. - **Rozvodna fotovoltaické elektrárny**, Opava – Kateřinky.
Příčina: v šetření.
Škoda: 1 000 000 Kč, požár likvidovaly 3 jednotky PO.

8. 4. – **Rozvodna velmi vysokého napětí**, Praha – Slivenec.
Příčina: v šetření.
Škoda – 8 250 000 Kč, požár likvidovaly 3 jednotky PO.

Policejní statistiky a jejich interpretace

Co se týče trestných činů souvisejících s elektrickou distribuční soustavou, jejich počet v meziročním srovnání mírně poklesl. V 1. pololetí 2014 **policie zaznamenala 490 případů, kdy byly objektem napadení rozvody elektrického proudu nebo trafostanice**. Ve srovnání se stejným obdobím roku 2013 se jednalo o pokles o 17,5 % (tehdy bylo zaznamenáno 594 případů). **Celkové škody dosáhly výše 34 823 600 Kč**. Také zde byl oproti roku 2013 zaznamenán pokles a to zhruba o 10 %.

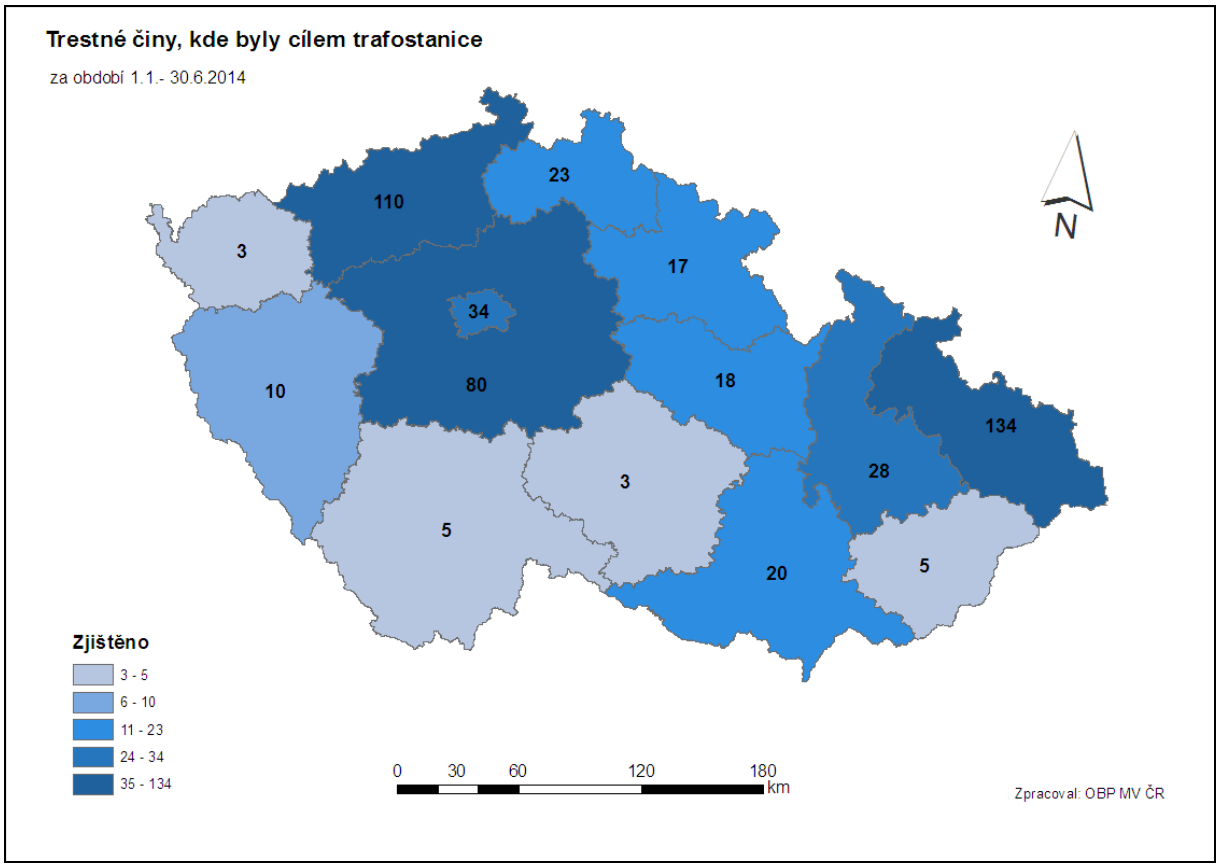


Z grafu je patrné, že v téměř dvou třetinách případů se ve vztahu k rozvodům elektrického proudu jednalo o trestný čin krádeže (krádež vloupáním 95 případů; krádež prostá 229 případů). Kradou se nejčastěji zpeněžitelné materiály – kabely, vodiče, elektroinstalační materiál, barevné kovy, oleje a pohonné hmoty. Započítány jsou ale také krádeže a ilegální odběry elektrické energie (135 případů).

Elektrická infrastruktura trpí také vlivem vandalismu. Bylo zaznamenáno celkem 30 případů sprejerství a 40 případů poškozování cizí věci. Zaznamenány byly také 4 požáry, které policie vyhodnotila jako přečin způsobený člověkem.

V 90 % výše uvedených případů se jednalo právě o přečiny. Přečinem se rozumí všechny nedbalostní trestné činy a dále ty úmyslné trestné činy, kde nehrozí trest odnětí svobody vyšší než 5 let. Jako zločin (tedy čin se sazbou vyšší než 5 let) byl skutek kvalifikován jen ve 49 případech.

Na níže uvedené mapě jsou znázorněny trestné činy v elektrické rozvodné síti dle jednotlivých krajů. Jak vidno, zdaleka nejhůře postižený je kraj Moravskoslezský, následovaný krajem Ústeckým. Regionální rozdíly jsou v tomto ohledu skutečně vysoké – vypovídající je srovnání kraje s nejvyšší incidencí (Moravskoslezský – 134 případů), s kraji s nejnižším počtem trestných činů (Karlovarský kraj a Vysočina zaznamenaly shodně pouhé 3 případy). Nízký počet činů v Plzeňském (10) 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.).



Je také zajímavé, že zatímco policie na Vysočině úmyslné poškozování elektrické rozvodné sítě téměř neeviduje, dle statistik Hasičského záchranného sboru (viz výše) patří tento kraj mezi nejpostiženější. Přírodní živly zde tak často nahrazují řádění člověka a celkové škody na elektrické infrastruktuře jsou tak v tomto kraji ve svém součtu přesto vysoké. Opět lze doplnit, že **Moravskoslezský kraj drží smutné prvenství ve statistikách policistů i hasičů**.

Velmi podobný obrázek získáme i v případě, pokud se podíváme na **ostatní objekty energetiky** (elektrárny, plynárny a rozvody plynu, uhelné doly atd.). Zde bylo ve sledovaném období **zaznamenáno celkem 100 trestných činů**. Nejčastěji šlo opět o trestné činy podvodu (§209; 52 případů) a krádeže (§205; 22 případů). Ve čtyřech případech policie zaznamenala havárie a provozní poruchy, způsobené lidskou nedbalostí, ve třech případech byl nicméně prokázán lidský úmysl. V oblasti teplárenství byl zaznamenán vůbec jediný trestný čin a to poškozování věřitele.

Celkové škody na ostatních objektech energetiky dosáhly výše 92 804 000 Kč. Z toho krádeže způsobily škody v objemu 1 727 800 Kč. Ačkoliv tedy tento typ trestného činu dominuje v celkovém počtu případů, zloději mají na svědomí jen zhruba 2 % celkového objemu škod. Drtivá většina škod byla zaznamenána v důsledku různých forem podvodů.

Není zřejmě překvapením, že celá jedna třetina těchto skutků se opět stala v Moravskoslezském kraji. Velmi dobře si naopak vedl kraj Karlovarský, kde byl zaznamenán jen jediný trestný čin. Zhruba 70 % zaznamenaných skutků tvořily přečiny, závažněji kvalifikované zločiny pak zbylých 30 %. Oproti elektrické infrastruktuře jsou tedy činy na ostatních objektech energetiky sice méně časté, ale obecně závažnější a s vyšší celkovou škodou.

Hlavní události a trendy v české a evropské energetice v I. pololetí roku 2014

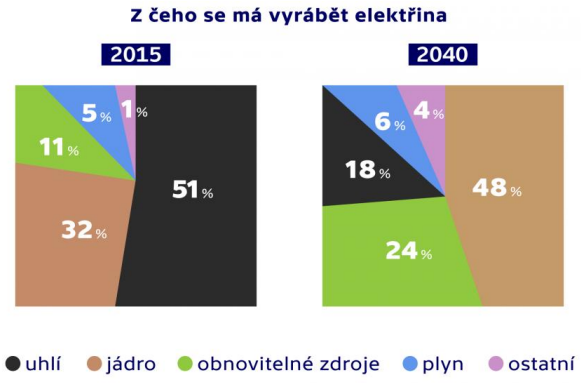
Energetika a energetická bezpečnost zůstávala jedním z hlavních témat veřejného diskursu i v prvních šesti měsících roku 2014. Vláda představila zcela novou energetickou koncepci, která do značné míry přehodnocuje dosavadní směřování a reaguje na nejnovější trendy. Jedním ze symbolů tohoto nového přístupu je i zastavení miliardového tendru na dostavbu jaderné elektrárny Temelín. Vývoj cen elektřiny totiž zpochybnil aktuální účelnost tohoto projektu. Česká republika se ovšem od jaderné energetiky neodklání, spíše naopak.

Ukrajinská krize nutí nejen ČR, ale celou Evropu zamýšlet se znovu nad spolehlivostí dodávek strategických surovin z Ruska. Po nedlouhé době se jedná o další připomenutí, že energetickou závislost lze snadno využít k politickému a ekonomickému nátlaku.

Nový směr pro českou energetiku

Rok 2013 byl pro Českou republiku v mnohém přelomový. Největší domácí energetický producent, společnost ČEZ, loni poprvé vyrobil více elektřiny z jádra než z uhlí. Tento fakt symbolicky reprezentuje postupnou změnu, kterou někteří analytici označují za konec „doby uhelné“. Ta u nás trvala řadu předchozích desetiletí.

Jak ukazuje následující graf, mnohaletou dominantní roli českých uhelných elektráren, dnes v čele s mohutným prunéřovským komplexem, má v budoucích dekádách převzít zejména výroba elektřiny z jádra. Do roku 2040 by se také měl více než zdvojnásobit podíl elektřiny vyrobené z obnovitelných zdrojů. Podíl uhlí by se měl zredukovat o celé dvě třetiny.



Zdroj: ceskatelevize.cz

Podobnou cestou opouštění uhlí jako hlavního zdroje (třebaže ne vždy za využití jádra jako náhrady) se vydává celá řada evropských zemí. Cílem je větší energetická nezávislost, diverzifikace energetického mixu a v neposlední řadě také snaha o zlepšení kvality ovzduší, které právě uhelné elektrárny zatěžují zdaleka nejvíce.

Nový energetický plán Ministerstva průmyslu a obchodu počítá s tím, že v roce 2040 se Česká republika stane z jednoho z největších vývozců elektřiny (v tuto chvíli je ČR dokonce pátým největším exportérem na celém světě) jejím importérem. Zatímco v současnosti prodáváme do zahraničí zhruba pětinu naší produkce (což odpovídá zhruba roční výrobě Temelína), v roce 2040 bychom už měli zhruba 5 % celkové spotřeby dovážet.

Jedná se hlavně o reakci na stále klesající ceny elektřiny, které souvisejí například i s celoevropským rozvojem obnovitelných zdrojů. Tento trend přitom bude v budoucnu pravděpodobně pokračovat. Náklady na to, aby si ČR zachovala své postavení předního exportéra, by tak mohly výrazně převýšit případné zisky z prodeje elektřiny do zahraničí.

Jednotný evropský energetický trh

EU přichází s dalším krokem na cestě k jednotnému evropskému trhu s energiemi. Evropská komise má v následujících dnech předložit návrh takzvaného síťového kodexu, který by měl lépe rozdělit přeshraniční kapacity přenosu energie a usnadnit tím vytvoření ničím nerušeného celoevropského trhu s elektřinou. Takové obchodování by podle EU mělo být rychlejší a ušetřit miliardy eur ročně.

V rámci dosavadní praxe musí výrobce elektřiny, který chce prodat své přebytky do zahraničí, získat i dostatečné kapacity na jejich přenos. Technické limity přenosových sítí ale neumožňují přeshraniční přenos dostatečného množství energie pro všechny, kdo o to mají zájem, takže přepravní kapacity se v současné době draží.

Nynější plán Bruselu by měl srovnat podmínky prodeje energie za hranice národních států. Na základě speciálně vytvořeného algoritmu by se na burze obchodovaly nabídky jednotlivých obchodníků v propojených trzích do výše dostupné kapacity pro přeshraniční přenos. Obchodníkům by se tím snížila rizika a nejistoty. Ti totiž často nevěděli, zda se jim podaří výhodně nakoupit energii a zároveň budou mít i kapacitu k jejímu přenosu. Na jednotném trhu však probíhá obojí automaticky - s jedním by bylo i druhé. Další výhodou by mělo být i optimální zapojení zdrojů do soustavy. Čím větší je oblast propojená pomocí přeshraničních kapacit, tím větší konkurence a také větší šance uplatnit případné přebytky elektřiny.

Cesta k úplnému propojení národních trhů ale bude ještě dlouhá. Původní odhady hovořily již o konci roku 2014, v současné době je ale jisté, že se bude jednat spíše o rok 2015. Propojení totiž musí předcházet sladění osmadvaceti různých systémů obchodování s energiemi, časů obchodování i konstrukce ceny. Je také nutné propojit různé IT systémy energetických burz a zajistit jejich vzájemnou kompatibilitu. Vedle toho je také potřeba vybudovat lepší přenosovou infrastrukturu a problémy činí i nestabilní obnovitelné zdroje.

Vytvoření jednotného trhu proto znamená investice v řádu milionů eur. O náklady na vznik a provoz systému by se přitom měli dělit provozovatelé jednotlivých národních burz a provozovatelé přenosových soustav. EU na něj neplánuje poskytovat žádné dotace.

O propojování trhů je mezi státy často zájem, spojit Evropu jako celek se ale dosud nikomu nepodařilo. Zatím existuje jen několik států, které s elektřinou obchodují mezi sebou – činí tak i Česká republika, která je součástí jednotného trhu se Slovenskem a Maďarskem. Propojení funguje i ve Skandinávii, mezi Španělskem a Portugalskem, spojena je také Itálie se Slovinskem či Německo, Belgie, Francie a Nizozemsko. V listopadu se pak plánuje propojení tohoto trhu se Skandinávií.

Evropská komise zároveň připravuje další změnu – využívání obnovitelných zdrojů má od roku 2017 fungovat na normálním tržním principu. Doposud se totiž obnovitelné zdroje ve většině států dotují. Pravidla mají platit od počátku července 2014. V letech 2015 a 2016 ale budou státy nový systém státní podpory prostřednictvím konkurenčního nabídkového řízení jen testovat u malé části své kapacity obnovitelných zdrojů. Teprve od roku 2017 se bude toto konkurenční nabídkové řízení vztahovat na veškerou výrobu.

Nový atomový zákon

V první polovině roku 2014 pokračovala příprava nové komplexní právní úpravy mírového využívání jaderné energie a ionizujícího záření. Nový atomový zákon má nahradit dosavadní zákon č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon).

Nová právní úprava odstraní nedostatky současného zákona zejména ve směru legislativně technickém a zahrne aktuální doporučení mezinárodních organizací (např. Mezinárodní agentury pro atomovou energii ve Vídni) a právní předpisy Evropského společenství pro atomovou energii (např. směrnice o ochraně před účinky ionizujícího záření). Návrh paragrafového znění nového atomového zákona byl připraven Státním úřadem pro jadernou bezpečnost ve spolupráci se zainteresovanými ministerstvy a dalšími institucemi již v roce 2013. V druhé polovině roku 2013 proběhlo meziresortní připomínkového řízení.

V první polovině roku 2014 probíhala vypořádání vznesených připomínek s jednotlivými resorty a dalšími institucemi (např. krajské úřady). Vzhledem k množství připomínek obdržených v meziresortním připomínkovém řízení a potřebě sladit návrh zákona s aktuálním stavem společného právního rámce EU, který se velmi dynamicky vyvíjí, bylo rozhodnuto, že v červenci 2014 proběhne další meziresortní připomínkové řízení a upravený návrh nového atomového zákona by měl být předložen do vlády v prosinci 2014.

Nový atomový zákon bude upravovat zejména:

- podmínky mírového využívání jaderné energie,
- podmínky vykonávání činností v rámci expozičních situací,
- nakládání s radioaktivním odpadem a vyhořelým jaderným palivem,
- schválení typu některých výrobků a podmínky přepravy radioaktivní nebo štěpné látky, radioaktivního odpadu a vyhořelého jaderného paliva,
- monitorování radiační situace,
- zvládání radiačních mimořádných událostí,
- podmínky zabezpečení jaderného zařízení, jaderného materiálu a zdroje ionizujícího záření (dále jen „zabezpečení“),
- požadavky k zajištění nešíření jaderných zbraní a
- výkon veřejné správy a kontroly v oblasti mírového využívání jaderné energie a ionizujícího záření.

Jednou z priorit Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030, která byla schválena usnesením vlády ČR ze dne 23. října 2014 č. 805, je širší zapojení právnických a podnikajících fyzických osob do přípravy na mimořádné události a krizové situace a jejich řešení cestou užší spolupráce s odpovědnými orgány veřejné správy a zvýšeným podílem na realizaci konkrétních úkolů u subjektů představujících zvýšené riziko pro své okolí. Atomový zákon proto ukládá povinnosti držitelům povolení včetně podílu na zajištění ochrany obyvatelstva v zóně havarijního plánování (jodová profylaxe, varování, preventivně výchovná činnost atd.).

Exkurz: Útoky na energetickou infrastrukturu

Tento exkurz se zaměřuje na příklady poškození či zničení kritické energetické infrastruktury, záměrně způsobené člověkem. Cílené útoky v oblasti energetiky jsou ve skutečnosti v Evropě velmi málo časté (jinak je tomu v některých jiných částech světa) a ani zdaleka se ve svém součtu nevyrovnají škodám, které energetikům působí přírodní vlivy (bouřky, mrazy, sucha, povodně atd.), případně technická selhání a nešťastné náhody. U mnoha škod sice lidský faktor negativní roli hraje, většinou se ale jedná o poškození z nedbalosti či např. zanedbání pravidelné údržby.

Jak velké riziko ale pro energetickou infrastrukturu představuje např. teroristický útok? Jak často k takovým incidentům dochází a jaké jsou škody? Může bezpečnost energetických provozů ohrozit kybernetický útok? A jsou akce ekologických aktivistů např. proti jaderným zařízením bezpečnostní hrozbou? Na tyto a další otázky se pokouší odpovědět následující stručná analýza.

Energetika a teroristé

O hrozbě teroristických útoků na kritickou energetickou infrastrukturu se v posledních letech hodně hovoří a píše. Někteří analytici označují nedostatečné zabezpečení těchto cílů za velkou potenciální hrozbu, přičemž je jen otázkou času, kdy jí teroristé využijí.

Ve skutečnosti ale známe ze současného západního prostředí jen velmi málo případů, kdy by se teroristé přímo zaměřili na energetické cíle. Ačkoliv závislost dnešní společnosti např. na dodávkách elektřiny a pohonných hmot je obrovská a jejich **dlouhodobější narušení by způsobilo rozsáhlé problémy, včetně ohrožení zdraví a životů velkého množství lidí**, pro nejznámější současné teroristické skupiny se zatím jedná o spíše méně lákavé cíle.

Hlavním záměrem teroristů je totiž působit na veřejné mínění, **šířit v populaci strach a paniku**. Teroristé pracují spíše s emocemi než s objektivními následky útoku. A tak zatímco je objektivním faktem, že rozsáhlý výpadek elektrické energie může v konečném důsledku způsobit daleko větší škody a mít za následek vyšší počet obětí než např. výbuch v metru či na letišti, traumatizující efekt na běžnou populaci bude ve druhém případě výrazně vyšší.

Pro příklady není nutné chodit daleko do minulosti. Útok na bostonský maraton si v roce 2013 vyžádal tři oběti. Po několik dní byl hlavním tématem mediálních výstupů doslova po celém světě a vyvolal obrovské množství reakcí. V červnu 2014 se po velké bouři ocitla bez elektrické energie velká část západní Austrálie a v přímém důsledku blackoutu (nikoliv bouře) zemřeli rovněž tři lidé, kterým se nedostala potřebná lékařská péče. S výjimkou australských médií o této události téměř nikdo neinformoval a i v samotné Austrálii byla tato zpráva spíše ve stínu jiných kauz (např. pátrání po zmizelém malajsijském letadle). Lze očekávat, že pokud by byl blackout způsobený teroristy, mediální zájem by byl o něco vyšší, i tak je ale nepravděpodobné, že by se byť jen blížil globálnímu pokrytí tragédie v Bostonu.

Útok hnutí FARC v Kolumbii

Bombové útoky či střelba na důvěrně známých místech, v dopravních prostředcích, školách, obchodních domech atd., obrázky zraněných či mrtvých, to vše je psychologicky (zejména v médiích) daleko působivější, než výpadek elektřiny nebo výbuch plynového potrubí v poli, jakkoliv může mít obojí nakonec stejné či větší následky. Úmrtí či zranění následkem blackoutu jsou totiž většinou „nepřímá“ a s teroristickým útokem souvisí jen zprostředkovaně. Hospodářské škody zase nevyvolávají zdaleka takové emoce, jako fyzické lidské utrpení. Totéž lze říci o útocích na produktovody, energetické závody atd. Pokud při útocích samotných přímo neumírají lidé, teroristé při nich nedosáhnou potřebného psychologického efektu. Např. blackout by musel být skutečně rozsáhlý a dlouhodobý, aby dosáhl stejného účinku na veřejné mínění, jako útok vedený „klasickými prostředky“ na „klasické cíle“.

Pro teroristy existuje jedna jediná podstatná výjimka, která má naopak potenciál vyvolat obrovské emoce dokonce i v případě, že útok bude nakonec málo ničivý. Touto výjimkou jsou jaderné elektrárny. Často podvědomý strach z radioaktivního záření a **nedůvěra k jaderné energii** jsou mezi lidmi velice rozšířené, což dokazují např. často přehnané reakce světové veřejnosti po havárii v japonské Fukušimě (hromadné nákupy jodových tabletek v Evropě a USA atd.). Některé státy na vlnu obav svých občanů dokonce reagovaly úplným odklonem od jaderné energetiky.

Jaderné provozy jsou pro teroristy sice lákavým, ale zároveň velmi obtížně napadnutelným cílem. Ve srovnání např. s dopravními prostředky představují typický „hard target“ – tyto objekty jsou velmi přísně střežené a chráněné. Případný útok má jen velmi malou naději ohrozit jadernou bezpečnost, naopak pro útočníky představuje jeho napadení značné riziko. Asi největší hrozbu představuje rozsáhlejší kinetický útok v kombinaci s „insiderem“ - pokud se teroristům podaří získat na svou stranu některého ze zaměstnanců elektrárny, jejich šance na úspěch se značně zvyšují. I tak ale bývají jaderné elektrárny místem, které jsou proti teroristickým útokům vůbec nejlépe zabezpečeny.

Z výše uvedených důvodů zůstávají známé teroristické organizace při výběru cílů spíše „konzervativní“ a raději zůstávají u běžných, osvědčených metod. V západním světě jsou teroristické útoky na energetickou infrastrukturu velmi řídké a častěji k nim dochází spíše v afrických zemích či na Blízkém východě, kde se např. ničení produktovodů často využívá jako forma nátlaku na místní vlády, které jsou na příjmech z prodeje energetických surovin zcela závislé. Navzdory tomu nelze tuto hrozbu podceňovat. **Právě fakt, že si západní státy uvědomují svou zranitelnost v této oblasti a cíleně pracují na tom, aby se z kritické energetické infrastruktury stal pro teroristy „hard target“, nejlépe přispívá k tomu, že se snižuje motivace těchto skupin se o podobné útoky pokoušet.** Navíc se v této oblasti objevují stále nové hrozby, z nichž zřejmě největší výzvu představuje možnost kybernetického útoku. Podcenit ale nelze ani tzv. osamělé vlky, kteří se mohou rekrutovat např. z řad nespokojených či propuštěných zaměstnanců energetických firem. Investice do zabezpečení kritické energetické infrastruktury jsou tedy nutné a samy o sobě vedou ke snižování rizika útoku i jeho případných následků.

Příklady útoků na energetickou infrastrukturu

V Evropě známe z minulosti příklad teroristické skupiny, která se při svých útocích zaměřovala primárně na energetickou infrastrukturu. Jednalo se o „**Výbor pro osvobození jižního Tyrolska**“ (BAS), skupinu německojazyčných radikálů, kteří se odmítali smířit s faktem, že toto území připadlo Itálii a požadovali jeho připojení k Rakousku. Od roku 1956 prováděli nekrvavé bombové útoky na sloupy elektrického vedení, ale také proti kasárnám a železničním tratím (před výbuchem vždy varovali, aby nedošlo ke zranění osob).

Jejich kampaň vyvrcholila při tzv. **noci ohně**, kdy se jim podařilo vyhodit do vzduchu celkem **37 sloupů vysokého napětí**. Jejich volba cíle nebyla náhodná – v podstatě celá severní Itálie tehdy byla (a tento stav částečně trvá dodnes) závislá na dodávkách elektřiny z Německa, přičemž značná část těchto velkých transportních kapacit byla vedena přes tyrolské horské průsmyky. Cílem BAS bylo rozsáhlým blackoutem ochromit severoitalský průmysl, a způsobit tak vládě v Římě tak velké ekonomické škody, aby souhlasila s jednáním o novém statusu jižního Tyrolska. To se do značné míry podařilo (škody byly obrovské a jižní Tyrolsko je dnes autonomní, dvojjazyčnou oblastí), kvůli opožděnému výbuchu jedné z náloží ale při akci tragicky zahynul jeden italský cestář. Teroristé později za tyto skutky (včetně obvinění z vraždy) stanuli před soudem a od 60. let je v oblasti klid.

Jaderná elektrárna Koeberg v JAR

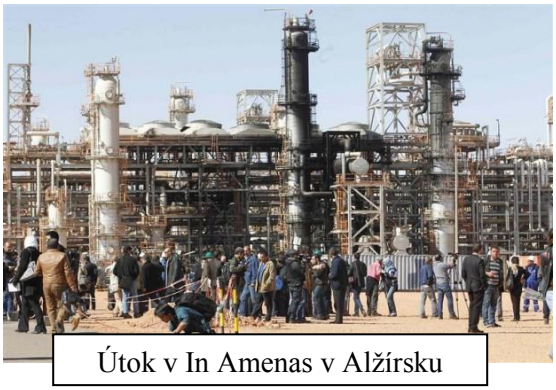
Jeden z mála případů „úspěšného“ teroristického útoku na jadernou elektrárnu se odehrál v jižní Africe. Skupina Umkhonto we Sizwe (což v jazyce zulu znamená „kopí národa“) byla ozbrojenou složkou Afrického národního kongresu Nelsona Mandely, která po masakru v Sharpeville začala používat teroristické metody v boji proti apartheidu. V roce 1982 se jí podařil **bombový útok na první jihoafrickou jadernou elektrárnu Koeberg**, která byla v té době ve výstavbě. Ačkoliv útok nemohl ohrozit jadernou bezpečnost (reaktor ještě nebyl dokončen), škody se vyšplhaly na 500 milionů randů (při dnešním kurzu přes 1 miliardu korun) a termín zprovoznění elektrárny se posunul o 18 měsíců.

Pokud se přesuneme do současnosti, pak zjistíme, že v posledních čtyřech letech se s útoky na svou kritickou infrastrukturu daleko více než evropské státy potýkaly USA. V roce 2013 došlo v Kalifornii k poměrně netradičnímu incidentu. Neznámý pachatel (spíše se jednalo o malou skupinu) zaútočil v noci **střelbou na** osaměle stojící **transformátorovou stanici poblíž San Jose**. Útočník nejprve před útokem přerušil optické kabely a následně začal z vyvýšeného místa ostřelovat jednotlivé transformátory, pravděpodobně z útočné pušky AK-47. Podařilo se mu rozstřílet nádrže na chladicí kapalinu u celkem 17 transformátorů, a vyřadit je tak z provozu v důsledku přehřátí. Při útoku sice nebyl nikdo zraněn, škoda na zařízení byla ale obrovská (zhruba 15 milionů dolarů, tj. přes 300 milionů korun) a pachatele se dopadnout nepodařilo. Útok ukázal na velkou zranitelnost menších energetických stanic, stojících často mimo obydlená místa. V současné době proto USA investují velké prostředky do jejich zabezpečení (kamerové a poplašné systémy atd.).

Ještě horší následky mohla mít **provizorní nálož, která v červenci 2014 vybuchla u malé elektrárny v Arizoně**. Nálož byla umístěna u dieselové nádrže s objemem 190 000 litrů. Pachatel naštěstí netušil, že nafta potřebuje mnohem vyšší zápalnou teplotu k tomu, aby explodovala, takže výbuch způsobil pouze její únik a elektrárna byla dočasně vyřazena z provozu. Útok ovšem nebyl veden zcela amatérsky, neboť podle FBI musel mít pachatel povědomí o režimu ochrany objektu a bombu umístil zřejmě při odchodu denní směny. V podezření se ocitla místní extremistická organizace „Fronta pro osvobození země“, někteří znalci ale tuto stopu zpochybňují a pachatel zůstává neznámý.

Za podobnými útoky často nestojí etablované mezinárodní teroristické skupiny, ale spíše vyšinutí jedinci, jejichž hlavním cílem je destrukce a vyšší politické cíle si obvykle nekladou. Příkladem může být **případ Johna Woodringa, který v roce 2013 spáchal v Arkansasu celkem tři útoky na energetická zařízení**. Poprvé se pokusil „zapřáhnout“ kabel vedoucí od sloupu vysokého napětí za jedoucí vlak s cílem zničit vedení. Ve druhém případě se mu podařilo založit oheň poblíž velkého výměníku, který tímto činem vyřadil z provozu a způsobil škodu 2 miliony dolarů. Nejzávažnější byl poslední incident, kdy pomocí traktoru porazil sloup vysokého napětí, a odřízl tak od energie více jak 9 000 odběratelů. Ani po Woodringově zatčení nebyl motiv jeho činů zcela objasněn.

K útokům na energetické cíle dochází pochopitelně mnohem častěji v oblastech zmítaných vnitřními ozbrojenými konflikty. Pro mnoho zemí je vývoz energetických surovin klíčovou součástí jejich hospodářství, a útok na toto odvětví tak může nejrůznějším ozbrojeným skupinám pomoci vytvořit silný tlak na místní vládu. Časté tak byly útoky separatistů z delty Nigeru, které se soustředily zejména na západní těžařské společnosti a docházelo při nich i k únosům jejich zaměstnanců. Velmi časté jsou útoky na ropovody a ropné rafinerie v Iráku – od pádu režimu Saddáma Husajna došlo již k několika desítkám různě závažných případů.



Útok v In Amenas v Alžírsku

Mezi nejrozsáhlejší ozbrojené útoky posledních let patří **obsazení plynařského komplexu poblíž města In Amenas** (na pomezí Alžírska a Libye) skupinou islámských radikálů s vazbami na Al-Kájdu. Několik desítek ozbrojených teroristů, kteří přijeli v dodávkách ze severního Mali, napadlo těžařské zařízení, které zčásti patří britské BP a norskému Statoilu a produkuje asi 10 % alžírského zemního plynu. Po několik dní zadržovali zaměstnance těžařských firem (bylo mezi nimi množství občanů evropských zemí) jako rukojmí – celkem se jednalo o více než 800 osob. Po čtyřech dnech vyjednávání došlo k tvrdému zásahu alžírské armády a speciálních jednotek, který si ale vyžádal životy 39 rukojmích. Zabito bylo také 29 teroristů, zbytek se stáhl zpět na území Mali, kde v současné době probíhá mezinárodní vojenská mise (i za české účasti), která má za cíl pomáhat místní vládě při potlačování těchto militantních skupin.

S útoky na energetickou infrastrukturu se v posledních letech ve velké míře potýká také Jemen, který se stal po pádu Tálibánu v Afghánistánu jedním z hlavních center zbytků Al-Kájdy. Začátkem roku 2014 v Jemenu proběhly dva závažné incidenty namířené na zneschopnění fungování elektrické sítě a přerušení dodávek ropy. Významné elektrárny a další energetické zařízení jsou umístěné v oblasti Marib, kde mají složky Al-Kájdy velkou sílu. Tato teroristická organizace prostřednictvím koordinovaných útoků ničí sloupy vysokého napětí, a přerušuje tak vedení energie do hlavního města San`á. V dané oblasti jsou podobné incidenty poměrně časté a způsobuji nedostupnost elektrického proudu pro miliony lidí.

Útoky na energetické cíle se nevyhýbají ani **Rusku**, zejména v neklidné oblasti Kavkazu. K **útoku na vodní elektrárnu** došlo v roce 2010 v kabardinsko-balkarské republice, poblíž města Baksan. V oblasti jsou ozbrojené útoky radikálů poměrně časté, nicméně tento incident se vymykal svou závažností. V časných ranních hodinách zaútočilo šest mužů na objekt elektrárny, přičemž zabili dva strážné a tři zranili. Poté připravili nálože a dálkově je odpálili. Přehrada sice nebyla sílou výbuchu ohrožena, ale elektrárna byla vyřazena z provozu. V Evropě byl zřejmě posledním rozsáhlým teroristickým útokem na energetickou infrastrukturu výbuch plynovodu na Ukrajině v červnu letošního roku. Ten zjevně souvisel s probíhajícím ozbrojeným konfliktem s proruskými separatisty a nedošlo při něm ke ztrátám na životech (více viz přehled událostí v této kapitole). Při válečných konfliktech je energetika logicky jedním z hlavních cílů, zřejmě nejničivější následky v tomto směru mělo zapálení kuvajtských ropných polí ze strany ustupující irácké armády během první války v Perském zálivu na počátku 90. let.

Další hrozby pro energetiku

Útok na kritickou infrastrukturu nemusí mít nutně kinetickou podobu. V posledních letech se v tomto ohledu stále častěji zmiňuje hrozba kybernetického útoku – **většina vyspělých energetických provozů a sítí se dnes neobejde bez sofistikovaných IT systémů, přičemž jejich kompromitace by mohla způsobit rozsáhlé škody**.

O kybernetických útocích se hovoří jako o jedné z hlavních hrozeb budoucnosti, neboť pro teroristy má tato forma napadení mnoho výhod – rychlost, nízké riziko dopadení, možnost

operovat na velké vzdálenosti, potenciálně značný ničivý účinek atd. **Velmi rizikový je v tomto ohledu opět lidský faktor**, představovaný zaměstnanci energetických firem. Právě ti disponují největší znalostí zranitelností v energetických systémech a mohou se (vědomě či nevědomě) na úspěchu případného útoku zásadně podílet.

Kybernetická ochrana energetické infrastruktury je důležitým tématem již nějakou dobu, k úspěšným teroristickým útokům v kybernetickém prostoru, které by měly větší dopad do hmotného světa, ale naštěstí zatím prakticky nedochází. V roce 2013 zveřejnily americké úřady zprávu o **sérii kybernetických útoků na řídicí systémy kompresorů, důležitých pro transport zemního plynu**. Při jejich ovládnutí by bylo teoreticky možné změnou tlaku v potrubí dovést zařízení až k explozi. Přestože byl útok veden hned na několik plynařských firem a je experty označován za poměrně sofistikovaný, nebyl natolik úspěšný, aby se mu podařilo způsobit reálné škody.

Energetické firmy jsou sice často terčem útoků hackerů, málokdy ale dojde ke skutečnému ohrožení samotných systémů. Jak jednoduché je vyvolat kybernetický incident dokazuje případ **Shamoon** z roku 2012. Tehdy byla vymazána veškerá data z 55 tisíc počítačů a serverů těžařských gigantů Saudi Aramco (v Saúdské Arábii) a Ras Gas (v Kataru). Smazání bylo důkladné a nenávratné – pachatel použil donekonečna se replikující obrázek, kterým přemazal všechny pevné disky (pokud by data jen odstranil, dala by se odborným zásahem obnovit). Jelikož byla tímto obrázkem americká vlajka, původně se spekulovalo o teroristickém útoku či politickém motivu, je ale možné, že za vším stál jen nespokojený zaměstnanec, který si veškeré informace, potřebné k vytvoření viru, našel na diskusních fórech na webu. Virus byl totiž přes svou účinnost velice primitivní. Ačkoliv naštěstí nebyly zasaženy žádné SCADA systémy (a nedošlo tak k žádnému poškození fyzické infrastruktury), ztráta dat znamenala pro obě firmy obrovskou škodu.

Velmi rizikový může být i dodávaný hardware a software, který může předem obsahovat „zadní vrátka“ (backdoor) k ovládnutí systému či počítačový virus. Příkladem může být slavná **špionážní aféra Farewell dossier z roku 1981**. Agent KGB Vladimír Větrov tehdy z ideologických důvodů zběhl a začal předávat velmi cenné informace francouzské tajné službě. Mimo jiné se tak Západ dozvěděl o operaci tzv. Ředitelství-T, skrze kterou se Rusové snažili dostat k vyspělým technologiím (především počítačovým mikročipům, polovodičům a SCADA systémům), což byla oblast, kde v 80. letech již Sovětský svaz výrazně zaostával.

Francouzský prezident Mitterrand nakonec o celé operaci řekl na setkání v Ottawě Ronaldu Reaganovi. CIA se následně rozhodla ruskou operaci nezastavovat a nechala Rusy krást falešné či upravené technické informace. Sověti více než rok podvod neodhalili a ukradené technologie se skutečně pokoušeli vyrobit a použít. Podle některých zdrojů způsobilo napodobování falešných amerických technologií velký výbuch transsibiřského plynovodu v roce 1982. Ve stejném roce ale Větrov spáchal ze žárlivosti vraždu a při výslechu vyšla najevo jeho práce pro západní tajné služby a byl následně popraven.

Pokud za výbuchem ruského plynovodu (o síle tří kilotun TNT) skutečně stály falešné americké počítačové komponenty, byl by to v podstatě první případ sofistikovaného (částečně kybernetického) útoku, který v mnoha směrech připomíná modus operandi viru Stuxnet, který byl v nedávné době použit na íránský jaderný program. V mnoha směrech je překvapivé, že záměrně dodaný falešný hardware a software zřejmě způsobil obrovské (a velmi „fyzické“) škody na kritické infrastruktuře. Právě Stuxnet je dalším příkladem velmi reálného poškození jaderného zařízení, které bylo způsobeno počítačovým virem.

Někdy jsou jako hrozba pro energetiku vnímáni ekologičtí aktivisté. Některé jejich akce (např. blokování vlaků přepravujících jaderný odpad) totiž často vedou k nemalým finančním škodám, které si většinou vyžádají rozsáhlé policejní zásahy. Na druhou stranu mají činy těchto organizací a jednotlivců většinou primárně demonstrativní charakter a nepředstavují přímou bezpečnostní hrozbu.

Příkladem může být novodobý trend pronikání do prostoru jaderných elektráren, které bývá doprovázeno vyvěšováním transparentů s hesly proti jaderné energetice. V roce 2013 se aktivistům hnutí Greenpeace podařilo úspěšně proniknout k budově reaktoru elektrárny Tricastin, v březnu 2014 se jim totéž podařilo u nejstarší francouzské jaderné elektrárny Fessenheim, zatímco prakticky ve stejnou chvíli se jejich kolegové ocitli za vnějším plotem švýcarské elektrárny Beznau I. Ve všech případech vyvěsili z těchto míst transparenty, upozorňující na rizika jaderné energetiky a následně byli zatčeni policií.

Ekologičtí aktivisté většinou prezentují tyto průniky jako příklad děravého zabezpečení těchto citlivých provozů a poukazují na to, že místo nich se mohl na střechu reaktoru stejným způsobem dostat například terorista. Skutečnost je ale taková, že při podobných akcích je výrazně preferována ochrana zdraví a životů všech zúčastněných (včetně samotných aktivistů), takže policie a ochranná služba elektráren často proti těmto lidem v první fázi aktivně nezasahuje, neboť po vyvěšení transparentů (a tedy splnění hlavního cíle své mise) často souhlasí s dobrovolným zatčením, což je varianta pro obě strany v zásadě přijatelná.

Tato metoda vychází z předchozích zkušeností, kdy při snahách zabránit aktivistům v průniku do prostoru elektrárny docházelo občas ke zraněním. Samotný pohyb osob v blízkosti vnějšího containmentu reaktoru nebo u chladících věží nepředstavuje sebemenší ohrožení jaderné bezpečnosti jako takové a elektrárna většinou kvůli těmto akcím nikterak nepřerušuje svůj běžný provoz. Je pochopitelné, že v případě útoku teroristů by byla reakce bezpečnostních složek zcela jiná, přičemž tyto scénáře jsou také pravidelně procvičovány (viz např. část věnovaná cvičení Safeguard Dukovany v této kapitole). Při těchto akcích je tak v ohrožení pouze mediální obraz provozovatelů elektrárny, nikoliv jaderná bezpečnost.

Cílem ekologických organizací pochopitelně nemusí být jen jaderné elektrárny. V květnu 2014 například členové Greenpeace vyvěsili transparenty za větší energetickou soběstačnost na plynové potrubí přes řeku Moravu na česko-slovenské hranici. Pokud při podobných akcích nedochází k poškozování daných zařízení, ale pouze k vyjádření názoru, není ze strany bezpečnostních složek důvod proti nim zasahovat.

Někdy ale akce aktivistů skutečně prokáží existenci bezpečnostních mezer. To je zřejmě případ **průniku skupiny odpůrců jaderného zbrojení do jinak přísně střeženého areálu Národního bezpečnostního komplexu Y-12 v Oak Ridge v Tennessee**. V těchto místech probíhá již od 2. světové války výzkum jaderných zbraní a nových metod využití jaderné energie. Trojici aktivistů se v roce 2012 podařilo dostat se přes vnější plot a bez povšimnutí se přes dvě hodiny pohybovat uvnitř areálu, kdy tento čas využili k potřísnění některých budov lidskou krví (akce se odehrála na výročí jaderného výbuchu v Hirošimě). Ostudu amerických bezpečnostních složek podtrhl především fakt, že všichni tři pachatelé byli v důchodovém věku, přičemž nejstarší z nich byla katolická jeptiška ve věku 84 let. Všichni byli odsouzeni k trestům vězení od tří do pěti let, jejich akce ale vedla k velkému zpřísnění ostrahy obdobných projektů po celých Spojených státech.

Kriminální motivy

V České republice se naštěstí s teroristickými útoky proti energetickým objektům prozatím nesetkáváme, **nemalé škody ale státu i energetickým firmám působí pachatelé s čistě kriminálními motivy (většinou zloději a vandalové)**. Fakt, že tito lidé nejsou motivováni politicky či nábožensky a jejich cílem je většinou jen zisk, je malou útěchou ve chvíli, kdy se škody jimi způsobené šplhají do desítek milionů, a úspěšně tak v tomto ohledu atakují některé teroristické činy známé ze zahraničí.

V minulé situační zprávě jsme například informovali o čtveřici pachatelů z Nového Jičína, kteří tak dlouho rozebírali sloupy vysokého napětí a prodávali jejich součásti do sběrny surovin, až dva z nich spadly a způsobily rozsáhlé výpadky v dodávkách pro několik tisíc domácností.

Poměrně časté jsou bohužel také krádeže olejů a dalších zpeněžitelných součástí z transformátorů. Nepoctivci se často obohatí o tisíce korun, ale **škoda na distribučním zařízení dosahuje na jednom kusu transformátoru cca půl milionu korun**. Téměř ve všech případech dochází k poškození životního prostředí - k úniku oleje do zeminy, kdy následně pak musí energetici provádět finančně i technicky náročné sanace půdy. Na pachatele zpravidla doplatí nevinní zákazníci, kteří jsou pak bez elektřiny do doby výměny zařízení. V neposlední řadě se pachatel vystavuje dosti značnému riziku zasažení elektrickým proudem.

Kromě izolačních olejů a vinutí transformátoru, které obsahuje barevné kovy, zloději kradou také měděné vodiče a nebrání se ani krádeži dvířek rozvaděčů nízkého napětí. K ohrožení života a zdraví tak může dojít u naprosto nevinných osob, zejména pak dětí, protože po odcizení dvířek jsou volně přístupné části pod napětím až do doby příjezdu poruchové čety. Především v těchto případech, kdy **následkem trestné činnosti vznikne hrozba zranění osob**, žádají energetici o spolupráci také veřejnost. Všichni pachatelé se přitom vystavují trestnímu stíhání. Při vyčíslení škody nad částku pět tisíc korun se již nejedná o přestupek, ale o trestný čin s odpovídající trestní sazbou.

To, že obyčejná krádež může často skončit obecným ohrožením, dokládá dvojice pachatelů z Klatovska. Ta v roce 2008 při krádeži mědi z trafostanice zřejmě omylem přepojila vodiče tak, že lidem v několika rodinných domech šlo krátce do zásuvek vysoké napětí. Škody byly naštěstí jen na spotřebičích a přenosové síti a k žádnému zranění tehdy nedošlo. Oba muže poslal soud do vězení. Ne vždy ale stojí za škodou snaha si vydělat - někdy to může být obyčejná touha po pomstě či závist. V červnu 2014 **navrtal neznámý vandal desítky děr do zcela nového teplovodu v Čáslavicích na Třebíčsku**. Škoda na zcela novém zařízení převýšila jeden milion korun. Někteří místní lidé jsou přesvědčeni o tom, že motivem činu byl fakt, že při stavbě teplovodu byli upřednostněni někteří zájemci před jinými. Kriminalisté tuto verzi ovšem zatím nepotvrdili. Pachateli v tomto případě hrozí až šest let vězení.

Kam až jsou někteří pachatelé ochotni zajít, dokazuje poměrně **extrémní případ z Mexika z loňského roku**. 28. října roku 2013 byla provedena série koordinovaných útoku na vysokonapěťové rozvodny v okolí mexického města Morelia. Tento útok způsobil výrazný blackout napříč státem Michoacan a způsobil nedostupnost dodávek elektřiny pro více než 400 000 lidí. Později se zjistilo, že tento útok měl za cíl pouze krýt přepadení 4 čerpacích stanic, ke kterým v nastalém zmatku došlo. Útok je připisován organizovanému drogovému kartelu Templářů (který bez návaznosti na rytířský řád, používá jejich název).

Cvičení BLACKOUT 2014

Ve středu 26. února po půl osmé ráno na několik sekund nečekaně zhasl celý pražský magistrát. Začalo tím hromadné cvičení simulující výpadek elektrického proudu, neboli blackout. Cvičení se účastnily orgány krizového řízení, bezpečnostní poradci, základní složky Integrovaného záchranného systému, Státní úřad pro jadernou bezpečnost, vybrané organizace a zahraniční hosté.

Příčina výpadku tak, jak ji simuloval pražský magistrát, zněla: část západní a celou střední Evropu už týden trápí silné bouřky a prudké elektrické výboje poškozují transformační stanice a vedení společnosti ČEPS na území Středočeského kraje. Následně je z provozu vyřazena transformační stanice Chodov a oprava si vyžádá minimálně několik dní. Selhala i snaha o náhradní napájení z rozvodny Malešice. Větrná smršť vyřadila z provozu i dvě funkční rozvodny PRE což mělo za následek i vyřazení rozvodny v Řeporyjích a následný blackout na celém území Prahy a v části středních Čech, například v okrese Kladno nebo Beroun.

Krátce po výpadku přechází důležité objekty na nouzový provoz ze záložních zdrojů. Má je například pražský magistrát nebo nemocnice. Značná část městské hromadné dopravy se zastaví, povrchovou dopravu začínají komplikovat nefunkční světelná signalizace a začínají se tvořit zácpy.

Podnětem ke cvičení byl především výpadek proudu z loňského června, kdy vyhořela rozvodna u Kunratického lesa a třetina Prahy se ocitla bez proudu. Podle Josefa Juránka, ředitele odboru bezpečnosti a krizového řízení magistrátu, je hrozba celkového blackoutu reálná i podle odborníků.

Závažný výpadek elektrické energie může znamenat ohrožení průmyslové výroby, dopravních systémů, omezení nebo přerušení dodávek pitné vody, plynu a tepelných energií, omezení telekomunikačního provozu a provozu výpočetních systémů, ale také zvýšení počtu negativních sociálních jevů, např. různých druhů kriminality. Měl by dopady i na peněžní trh z důvodu nefunkčnosti bankomatů a na zásobování potravinami.

V závěrech cvičení Blackout je podle pražského magistrátu navrženo 32 konkrétních doporučení ke zlepšení současného stavu, které budou uloženy jednotlivým zástupcům MHMP a složkám IZS a šest návrhů na zlepšení, které chce Praha předložit Bezpečnostní radě státu. Praha také na základě výsledku cvičení zvažuje vybudování záložní elektrárny, která by v případě výpadku byla schopná pokrýt zhruba třetinu spotřeby elektřiny v metropoli.

Důležité je ale pro případný záložní zdroj zajistit potřebné finance a shodnout se na vhodné lokalitě. Dle některých expertů může tento záměr narazit na odpor místních obyvatel. Myšlenka na vznik záložního energetického zdroje pro případ výpadku proudu se v Praze neobjevuje poprvé. Už v roce 2010 Pražská energetika zvažovala stavbu plynové rychlonabíhací elektrárny v Bohnicích.

Cvičení SAFEGUARD
Dukovany 2014

Cvičení mělo prověřit součinnost Armády České republiky, Vojenské policie, Policie České republiky a pracovníků Jaderné elektrárny Dukovany při vnější ochraně Jaderné elektrárny Dukovany. Do cvičení se zapojilo také dvacet policistů Krajského ředitelství policie kraje Vysočina, včetně speciálně vycvičených příslušníků zásahové jednotky pro ochranu Jaderné elektrárny Dukovany. Uskutečnilo se ve dnech 30. května až 3. června 2014.

Cvičení bylo připraveno v souladu s doporučením Evropské komise a programy zvyšování bezpečnosti jaderných zařízení a navazuje na obdobné loňské cvičení SAFEGUARD 2013 uspořádané při Jaderné elektrárně Temelín. Celé cvičení vyvrcholilo součinnostními ukázkami v pondělí 2. června 2014, při kterých společně vojáci a policisté reagovali na různé varianty simulovaného napadení elektrárny. Do cvičení se zapojily i vrtulníky z 22. základny vrtulníkového letectva Sedlec, Vícenice u Náměště nad Oslavou, psovodi a pyrotechnici Vojenské policie.

Do pondělních šesti dynamických ukázek se zapojilo 64 příslušníků 191. pěší roty aktivní zálohy, která působí při Krajském vojenském velitelství v Jihlavě, a jejichž velitelem je nadporučík Karel Hanák. Ten uvedl, že jeho jednotka se do prostoru elektrárny přesunula už v pátek 30. května z Vojenského újezdu Boletice, kde plnila úkoly bojové střelby, jimiž končí tříletý výcvikový cyklus aktivní zálohy. *„Tady jsme postupně vybudovali kontrolně propouštěcí místa a začali střežit přístupové cesty i vodní zdroj, který je pro chod elektrárny nezbytný. Dnešní ukázky, které jsme připravili ve spolupráci s dalšími složkami IZS, už jsou jen jakousi třešinkou na dortu,“* konstatoval Hanák a zdůraznil, že prioritním posláním jednotek aktivní zálohy je právě střežení a ochrana objektů zvláštní důležitosti.

Vybrané události ve sledovaném období

Leden

V Pardubicích instalují kvůli zlodějům kovů nové kryty sloupů elektrického osvětlení
Počet krádeží krytů pouličních lamp donutil místní zastupitele k jejich postupné výměně za nový, pro zloděje méně lákavé typ. Sloupy s odkrytými dráty vysokého napětí jsou totiž velmi nebezpečné - kdyby proud někoho zranil, krádež kovových dvířek by se rázem z přestupku stala trestným činem. Staré lampy tak z ulic postupně mizí. Některá města, např. Bohumín, výkup železného šrotu na svém území zakázala úplně. Lidé mohou železo odevzdávat zdarma ve sběrných dvorech, odkud jej teprve mohou vykupovat sběrny formou dražby.

Únor

Výbuch plynu zničil dům v Ostravě
Velká exploze v únoru zcela zničila rodinný domek v Ostravě-Martinově. Hasiči, policisté i záchranáři byli na místě během několika málo minut a podařilo se jim z trosek vyprostit těžce zraněného majitele, který musel být po převozu do nemocnice uveden do umělého spánku. Výbuch rozmetal trosky domu po okolních zahradách.

Možnou těžbu břidlicového plynu na Náchodsku zastavilo Ministerstvo životního prostředí
Cesta k těžbě břidlicového plynu na severovýchodě Čech se zavírá. Těžaři měli zájem o těžbu na Trutnovsku a Náchodsku a požádali ministerstvo životního prostředí o povolení průzkumu. Ministerstvo ale řízení o stanovení průzkumného území zastavilo. Ačkoliv těžební společnost Basgas Energia Czech postupně omezila původní záměry na rozsah průzkumu tak, aby se vyhnula chráněným územím a území ochrany vod, proti možné těžbě se zvedl velký odpor místních, kteří se obávali zničení krajiny a kontaminace pitné vody. Společnost chtěla pro těžbu využít metodu hydraulického štěpení.

Kvůli úniku plynu hasiči ve Vyškově evakuovali školu a kino
Na místě zasahovalo pět jednotek hasičů. Ti museli evakuovat zhruba 270 lidí, včetně 80 dětí z blízké základní školy v ulici Tyršova. Evakuováno bylo i kino a bytový dům. K havárii došlo vinou plynařů, kteří na místě pracovali na plynové přípojce. Ti omylem porušili potrubí. Únik plynu se podařilo v pozdních odpoledních hodinách zastavit. Plynaři díru za asistence hasičů zacelili a krátce po 17. hodině se lidé mohli vrátit do svých domovů.

Pokračující problémy ČEZu a Energo-Pro v Bulharsku
Krátce poté, co v Bulharsku skončily nepokoje kvůli drahé elektřině, přicházejí pro zahraniční investory další problémy. Rakouská EVN a české firmy ČEZ a Energo-Pro, jsou pod tlakem, který na ně skrz ultimátum vyvíjí tamní ministerstvo energetiky. To požaduje uhrazení dlužných poplatků ve výši 318 milionů leva (4,4 miliardy korun) státní energetické společnosti NEK. Jinak mohou firmy přijít o licence. ČEZ a EVN jakékoliv provinění odmítají a tvrdí, že NEK jim naopak nevyplatil peníze, které jim ze zákona má vyplatit za instalaci větrných a solárních elektráren. Takový krok by byl další ranou pro zahraniční investory v energetickém sektoru, které již zasáhlo rozhodnutí socialistické vlády dvakrát snížit domácnostem účty za elektřinu. Snížením cen elektřiny chtěla vláda zabránit protestům veřejnosti kvůli vysokým účtům, které ujídaly velkou část příjmů domácností.

Italská skupina Tamini získala zakázku na ochranu ČR před blackouty

Skupina Tamini vyhrála tendr na výstavbu dvou transformátorů na hranicích s Německem, které mají bránit českou síť před velkými přetoky elektřiny z německých větrných elektráren na severu země. Italové vyhráli díky ceně. Tamini nabídla jednu miliardu korun, což bylo výrazně méně, než požadovala konkurence. Porazila Siemens, Alstom nebo ABB. U hranic s Německem má do konce roku 2016 postavit dva stroje na regulaci elektrického proudu. Tendr vypsala a financuje společnost ČEPS, provozovatel české přenosové soustavy.

Transformátory mají být uvedeny do provozu na konci roku 2016. Stroje na regulaci toku elektrického proudu do Česka budou postaveny dva. Oba se budou nacházet v rozvodně Hradec u Kadaně. Miliardu stojí jen samotná zařízení. Celá výstavba vyjde ČEPS na více než dvě miliardy korun, projekt totiž zahrnuje také např. výkupy pozemků, terénní práce atd. Hlavním důvodem pro výstavbu transformátorů je hrozba blackoutu, s níž se Česko v uplynulých letech několikrát setkalo, naposledy v létě loňského roku. Blackout nastává, když nekontrolované přetoky elektřiny naruší síť tak, že se kvůli ochraně začne sama vypínat.

Důvodem těchto přetoků jsou hlavně německé slunečné a větrné elektrárny na pobřeží Severního a Baltského moře. Elektřina z nich putuje na jih země, kde je soustředěn průmysl. Německá přenosová infrastruktura však na tyto toky nestačí, proto na jih země cestuje německá elektřina přes Česko, čímž občas dochází k nekontrolovaným přetokům.

Rozsáhlá rekonstrukce elektrického vedení na Královéhradecku

Časté výpadky elektřiny a přetížené vedení vysokého napětí trápí okrajové části Hradce Králové a okolní obce. Energetici se proto pustí do rozsáhlé opravy. Rekonstrukce má posílit elektrické vedení v lokalitách, kde přibývá rodinných domků nejvíc. S podobnými problémy se potýkaly i severní Čechy, tam ČEZ nedávno dostavěl nové vedení za 100 milionů, o kterém jsme informovali v minulé situační zprávě. Zbývá na něj napojit ještě Šluknovský výběžek. Problém je ale v tom, že stožáry se mají stavět v chráněném území Lužických hor, proti čemuž místní protestují.

Oprava bude stát 32 milionů korun, ale měla by podle společnosti ČEZ přinést omezení poruchovosti a zvýšení spolehlivosti dodávek elektrické energie. Posílit zásobování proudem potřebuje také Šluknovský výběžek. Energetici ho chtějí napojit na vedení z Nového Boru přes Svor a Varnsdorf. "Chceme docílit stabilizace dodávek a posílit jejich spolehlivost. Česká republika je jedním z nejlépe zasíťovaných území v rámci celé Evropy. Do jednoho místa dokážeme přivést napájení z více zdrojů - to ale neplatí právě v případě Šluknovska," vysvětlil České televizi mluvčí ČEZu Jan Pavlů. Kvůli sloupům by se však musel vykácet osmnáctikilometrový pás lesa v šířce 30 metrů v Chráněné krajinné oblasti Lužické hory. Místní obce proto požadují, aby vedení bylo vedeno v zemi. V současné době je snaha najít kompromis, neboť i podzemní vedení je v mnoha ohledech problematické.

Cvičení simulovalo blackout všech čtyř bloků Dukovan

Ve čtvrtek 13. března se v JE Dukovany uskutečnil historicky první blackout (ztráta elektrického napájení), jenž se týkal všech čtyř bloků, při kterém došlo k úplnému odpojení elektrárny od vnější sítě. Šlo sice o cvičení, ale právě jeho průběh poskytl neocenitelné informace pro jeho úspěšné zvládnutí. Akce proběhla ve spolupráci s příslušnými síťovými pracovišti (dispečinky, rozvodnami, vodními elektrárnami). Přínosy těchto cvičení potvrdila již v minulosti mezinárodní mise OSART a zařadila je mezi tři nejvýznamnější dobré praxe na EDU.

Extrémní nárazový vítr, násobení poruch v propojených napěťových soustavách a rostoucí frekvence jsou předzvěstí událostí, které jsou černou můrou pro všechny energetiky. Působením silného větru dochází k pádu stožáru rezervního vedení 110 KV, následuje výpadek rozvodny 400 kV Sokolnice. Dochází k dalšímu vypnutí vedení a EDU se nachází v tzv. Ostrovním provozu. Nastává tzv. blackout na všech čtyřech blocích jaderné elektrárny, který je charakterizován jako nadprojektová havárie a směnový inženýr vyhlašuje „Stav nouze“.

V tomto okamžiku přichází chvíle pro ověření chodu dvou plánovaných dieselagregátů AAC DG, díky kterým se postupně daří obnovovat napětí na jednotlivých rozvodnách elektrárny a ukončovat tak beznapěťové stavy na jednotlivých blocích 1,3 a 4. Nové dieselagregáty budou instalovány na základě doporučení výsledků tzv. stresstestů, které hodnotily provoz elektrárny z pohledu vlivu extrémních klimatických podmínek v závěru tohoto roku. Pro lepší procvičení komunikace s vnějšími subjekty je ve scénáři zařazena obnova napětí na 2. bloku EDU z Dalešic a podání záložního napájení z Vranova do Slavětic.
Na průběh celého cvičení dohlíželi inspektoři SÚJB, kteří v Dukovanech provádí oficiální inspekci, která je zaměřena na ověření plnění požadavků Atomového zákona a jeho prováděcích předpisů.

Duben

Výpadek proudu v Praze kvůli technické závadě na rozvodně Chodov
Dodávka elektřiny byla obnovena po zhruba deseti minutách, výpadek ale zasáhl v podstatě celou jižní část metropole. Zařízení na Chodově je místem, kde proud odebírá Pražská energetika z nadřazené energetické soustavy. V rozvodně, která patří firmě ČEPS, se pak napětí transformuje na nižší. V červnu roku 2013 došlo ve stejné rozvodně k výbuchu transformátoru, který způsobil více než dvouhodinový výpadek. K menší závadě došlo také v srpnu loňského roku, kdy kvůli přerušení dodávky několik minut nejezdily v části Prahy tramvaje ani metro.

Zlepšení ovzduší slibuje nová plynová kotelna v Proboštově
Významnou investiční akci za více než 160 milionů korun realizuje v současné době v Elektrárně Ledvice ČEZ Teplárenská, a. s., ze Skupiny ČEZ. Jedná se o výstavbu největší plynové kotelny v České republice, která nahradí výtopnu v Proboštově. Kotelna se svými čtyřmi kotli na zemní plyn bude schopna vyrobit 200 tun ostré páry hodinově. Kotelna bude schopna fungovat jako dostačující záložní zdroj výroby tepla pro Bílinu, Teplice a Ledvice. Zároveň bude podpůrnou složkou pro vysoce ekologický nový zdroj o výkonu 660 MW při jeho najíždění do provozu po případných odstávkách.
Podle dohody s výrobcem budou kotle naloženy v Norimberku na loď a po Dunaji se dostanou až do Bratislavy. Tam budou přeloženy na „kola“ a po silnicích různých tříd se následně dostanou až do Ledvic. Jedním z hlavních důvodů investice je snížení emisní zátěže v regionu. Díky nové plynové kotelně tak poklesnou emise SO_2 o 114 tun, NOxo 16 tun a tuhých znečišťujících látek o 350 kilogramů ročně. 34 procent cílové částky je hrazeno z Fondu soudržnosti Evropské unie.

Začala stavba ventilátorových věží, které zvýší bezpečnost JE Dukovany
Mezi finančně i organizačně nejnáročnější opatření, která vyplynula ze stresstestů po havárii jaderné elektrárny v japonské Fukušimě, patří výstavba koncového jímače tepla, tzv. ventilátorových věží v Jaderné elektrárně Dukovany. Ty jsou odolné proti zemětřesení, tornádu, přívalům deště i sněhu. Hodnota investice představuje stovky milionů Kč (cca 800 – větší část investice bude uložena pod zemí, menší část ventilátorové věže, bude viditelná nad zemí).
Stavební povolení ke stavbě těchto nízkých extrémně odolných ventilátorových věží, určených především ke chlazení bezpečnostních systémů elektrárny, obdržela Jaderná elektrárna Dukovany od MPO ČR v srpnu 2013. Dokončení objektu o velikosti 27mx40mx17,5m a jeho připojení na navazující potrubní trasy a kabelové kanály pro 1. a 2..blok elektrárny proběhne v roce 2015. Druhý identický objekt, blok šesti ventilátorových věží pro chlazení tří bezpečnostních systémů 3. a 4. bloku JE Dukovany, bude dokončen a připojen v roce 2016 na východním konci elektrárny.

Ventilátorová věž je betonový skelet, odolný proti zemětřesení, vyzbrojený 6 kusy ventilátorů o průměru 8 metrů. Celkový výkon pro chlazení je 88 MW tepla. Provozní režim ventilátorů umožňuje kromě dvou stupňů otáček také tzv. reverzní chod, který lze využít proti zamrzání ventilátorů a rozstřikovacích trysek při extrémně mrazivém počasí.
Současná osmice chladících věží zůstane dominantou elektrárny a bude fingovat jako dosud pro chlazení kondenzátorů turbín.

Květen

Hasiči nacvičovali záchranu osob ze stožárů velmi vysokého napětí
Cvičení Portál 2014 simulovalo situaci, v níž uvízly dvě osoby na stožáru velmi vysokého napětí. Mělo prověřit spolupráci bezpečnostních pracovníků společnosti ČEPS a všech složek integrovaného záchranného systému. Na akci se podílela i helikoptéra Letecké služby Policie České republiky a lezci z hasičské stanice Krč a Smíchov. Celá akce trvala zhruba 70 minut.

Policie chytila čtyři zloděje oleje z transformátorů
Policii ČR se v květnu podařilo zadržet skupinu pachatelů, která se doznala k několika krádežím olejové náplně z distribučních transformátorů v oblasti Karvinska a částečně i Frýdecko-Místecka. Tato čtveřice byla následně ostravským Okresním soudem odsouzena k trestům odnětí svobody a náhradě škody ve výši cca 100 tisíc korun.
Společnost ČEZ Distribuce eviduje ročně desítky případů krádeže vinutí transformátoru i jeho olejových náplní. Zloději ve snaze o dosažení rychlého a snadného zisku hazardují se svými životy, kdy jim hrozí při zásahu elektrickým proudem smrtelná poranění, případně těžké popáleniny s doživotními následky. Energetici zintenzivnili spolupráci s Policií ČR v lokalitách, kde se krádeže vyskytují, a ta je stále úspěšnější v odhalování těchto činů.

Cvičení úniku ropných látek v elektrárně Počerady

Ropné látky unikly ve středu 14. května do vodoteče Elektrárny Počerady. Stalo se tak během čištění nádrže gravitačního odolejovače. Pracovník obsluhy o této mimořádné události okamžitě informoval směnového inženýra a ten ohlašovnu požáru elektrárenského hasičského záchranného sboru. Vzápětí se rozjel nezbytný kolotoč obnášející svolání členů havarijního štábu, vyhodnocení situace a samozřejmě i samotný výjezd hasičů k vyústění vodoteče do Počeradského potoka. Zatímco se nad elektrárnou nesly tóny havarijní sirény, byli všichni její zaměstnanci prostřednictvím místního rozhlasu informováni, že se jedná o cvičení, jehož účelem je ověření havarijní připravenosti všech dotčených složek.
Havarijní cvičení se v elektrárnách Skupiny ČEZ konají každoročně. Letos jich bude celkem 23, z toho 14 v klasických a 9 ve vodních elektrárnách. Na severu Čech má tak za sebou ověření havarijní připravenosti již Elektrárna Ledvice, i zde se jednalo o simulovaný únik nebezpečných látek do vodoteče. Ostatní severočeské hnědouhelné elektrárny čeká podobná událost na podzim.

Červen

Orlík na zkoušku napájel temelínská čerpadla
Vodní elektrárna Orlík v červnu zásobovala hodinu elektřinou jadernou elektrárnu Temelín. Energetici si tím vyzkoušeli, jestli Orlík dokáže zajistit chod bezpečnostních systémů Temelína v případě výpadku proudu. Termín testů se plánoval s ohledem na odstávku prvního bloku Temelína. Proud z Orlíku v Temelíně využili k najetí čerpadla cirkulační chladicí vody, které se svým výkonem patří k největším na elektrárně. Testu se účastnili pracovníci společností ČEZ, E.ON a ČEPS.

Pokud by přenosovou soustavu postihl výpadek proudu a temelínským technikům by se nepodařilo zajistit elektřinu z dalších záložních zdrojů, právě Orlík nebo Lipno by Temelínu dodávaly elektřinu pro zajištění chlazení. Jako první na řadu přišlo Lipno. "Deset procent výkonu jednoho ze dvou lipenských turbogenerátorů je dostatečných, aby Temelín měl potřebné množství elektřiny pro chlazení reaktoru. Tato zkouška už proběhla před několika lety. Teď jsme si ověřili i severní variantu s výkonově silnějším Orlíkem," uvedl pro Českou televizi ředitel Vodních elektráren ČEZ Petr Maralík.

Masivní únik plynu uzavřel ulici v Brně

Kvůli závadě plynovodu musela být celý jeden den uzavřena pro chodce i automobily Měřičkova ulice v Brně-Řečkovicích. Plyn unikal ve velkém množství do kabelové šachty, odkud jej odvětrávali hasiči, zatímco policie uzavřela průchod ulicí. Evakuace obyvatel nebyla nutná, nedošlo k výbuchu ani ke zranění osob.

Na východě Ukrajiny explodoval plynovod

V Poltavské oblasti na východě Ukrajiny vybouchl plynovod, ve kterém se přepravuje plyn ze Sibiře do Evropy. Při výbuchu nebyl nikdo zraněn, vzhledem k nestabilní situaci v zemi je jako příčina nejčastěji zmiňován teroristický útok. Rozsah dodávek plynu do EU nebyl událostí nikterak narušen. K výbuchu, po němž podle očitých svědků šlehaly plameny do výše 200 metrů, došlo u města Lochvycja, ležícího asi 200 kilometrů východně od Kyjeva. Úsek plynovodu Urengoj-Pomary-Užhorod se nachází asi kilometr od obytných stavení. Plynovod Urengoj-Pomary-Užhorod byl letos už jednou poškozen, když u něj v květnu explodovala nálož v Ivano-Frankivské oblasti na západě země. K výbuchu došlo daleko od Doněcké a Luhanské oblasti, kde už řadu týdnů trvají boje mezi armádou a proruskými povstalci. Potrubí překračuje rusko-ukrajinskou hranici v Sumské oblasti na severovýchodě Ukrajiny a opouští ji v Užhorodě. Odtud plyn směřuje dál na západ přes kompresorové stanice na hranicích se Slovenskem, Maďarskem a Rumunskem.

ČEZ uzavřel s Albánií dohodu o narovnání

Společnost ČEZ podepsala ve Vídni pod dohledem Sekretariátu energetického společenství dohodu o narovnání s albánskou stranou. Podle dohody získá ČEZ, po splnění odkládacích podmínek, v ročních splátkách celkem 100 milionu EUR, tedy částku obdobnou počáteční investici do nákupu albánské distribuční společnosti. Součástí dohody jsou i podmínky ukončení sporu před mezinárodním arbitrážním soudem. „Sjednanou dohodu považuji za úspěch zejména vzhledem k tomu, že se získanými finančními prostředky budeme moci disponovat výrazně dříve, aniž bychom museli čekat řadu let na výsledky arbitráže. Dohoda je koncipována tak, že finanční kompenzace bude zajištěna renomovanou evropskou bankou," uvedl Daniel Beneš, předseda představenstva a generální ředitel ČEZ, a. s.

Podle uzavřené dohody obdrží ČEZ za úhradu pohledávek a převod podílu v CEZ Shpërndarje kompenzaci 95,5 milionů EUR, dalších 4,5 milionu EUR již Skupina ČEZ obdržela. Částka bude vyplácena v ročních splátkách do roku 2018. Dohoda je podmíněna splněním několika odkládacích podmínek. Mezi ně patří vystavení bankovní garance, schválení dohody albánskou vládou a následná ratifikace albánským parlamentem. Na straně ČEZ je potřebné schválení dohody statutárními orgány společnosti. Společnost ČEZ vstoupila na albánský trh v roce 2009. Investice do koupě distribuční společnosti představuje 3,6 % celkových investic do zahraničí a méně než 1 % z celkových investic Skupiny ČEZ v letech 2005 – 2011.

***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,*

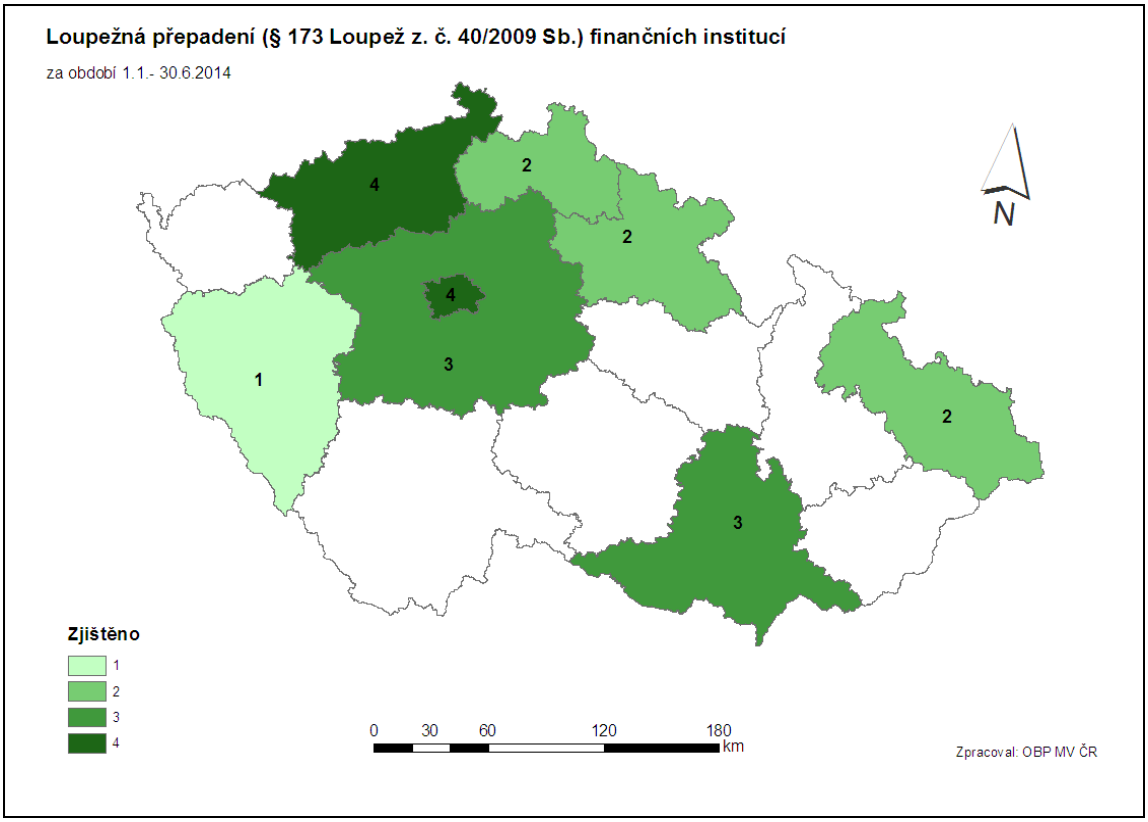
BEZPEČNOST FINANČNÍCH INSTITUCÍ

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 **loupeže**. Následovat budou další formy trestné činnosti od skimmingu, přes úvěrové a pojistné podvody. Nakonec věnujeme pozornost jednomu z fenoménů současnosti – virtuálním měnám a jejich bezpečnostním rizikům.

Dobrou zprávou je, že ve srovnání s rokem 2013 **počet loupežných přepadení bank a finančních institucí v České republice výrazně klesl**. Meziroční pokles byl téměř třetinový (30,3 %). V období **od ledna do února 2014 se jich událo celkem 21**. Do této chvíle se podařilo dopadnout pachatele v sedmi případech, tedy přesně ve třetině celkového počtu. Objasněnost tohoto typu kriminality je nicméně vysoká – 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 výrazně vyšší.

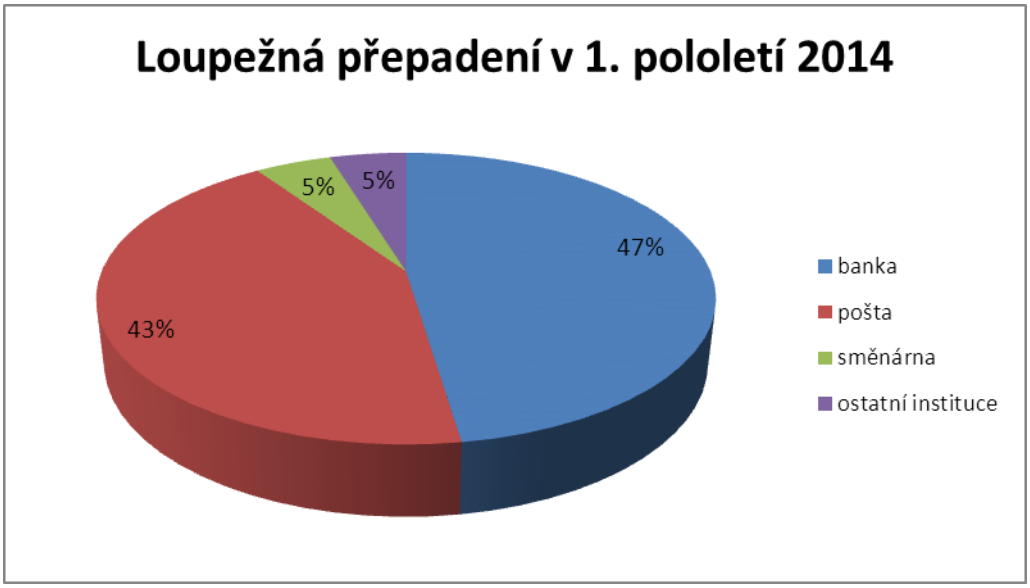
Tento typ trestné činnosti nabývá velmi často sériového charakteru – pachatel je mnohdy nadšen počátečním úspěchem a poměrně záhy se pokusí si tímto „snadným“ způsobem vydělat další peníze. V naprosté většině případů tak lupič dříve či později skončí v policejních poutech. Nejčastěji se přitom jedná o lidi, kteří se k tomuto činu zpočátku uchylují kvůli dluhům, které již nejsou schopni splácet. Ani úspěšné přepadení banky přitom dluhovou spirálu většinou neukončí, protože pachatelé získané finance záhy utratí.



Z mapy vyplývá, že v uplynulých šesti měsících došlo k nejvíce přepadením (4) v Praze a v Ústeckém kraji. 3 případy zaznamenal také Středočeský a Jihomoravský kraj. V šesti krajích (Olomoucký, Zlínský, Jihočeský, Karlovarský, Vysočina, Pardubický) se přitom v prvním pololetí roku 2014 žádné loupežné přepadení finanční instituce neodehrálo. **Pachatelé si celkem odnesli 1 365 900 Kč**.

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 často odehrává 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).

Nárůst případů v uplynulých letech byl dáván do souvislosti s ekonomickou krizí a zhoršenou finanční situací řady obyvatel. Lze očekávat, že se v případě zlepšení celkové ekonomické situace a obnovení hospodářského růstu sníží i incidence tohoto negativního společenského jevu. V rámci zlepšování objasněnosti tohoto druhu kriminality je 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.



Z výše uvedeného grafu je zřejmé, u jakých objektů dochází k loupežným přepadením nejčastěji. S mírným náskokem vedou bankovní pobočky, velmi lákavé jsou pro lupiče také pošty. K přepadení směnáren a dalších zařízení naopak dochází méně často. Za rok 2013 byla přitom dominance bank daleko patrnější – odehrálo se v nich celých 54 % loupežných přepadení (pošty tvořily jen 27 %).

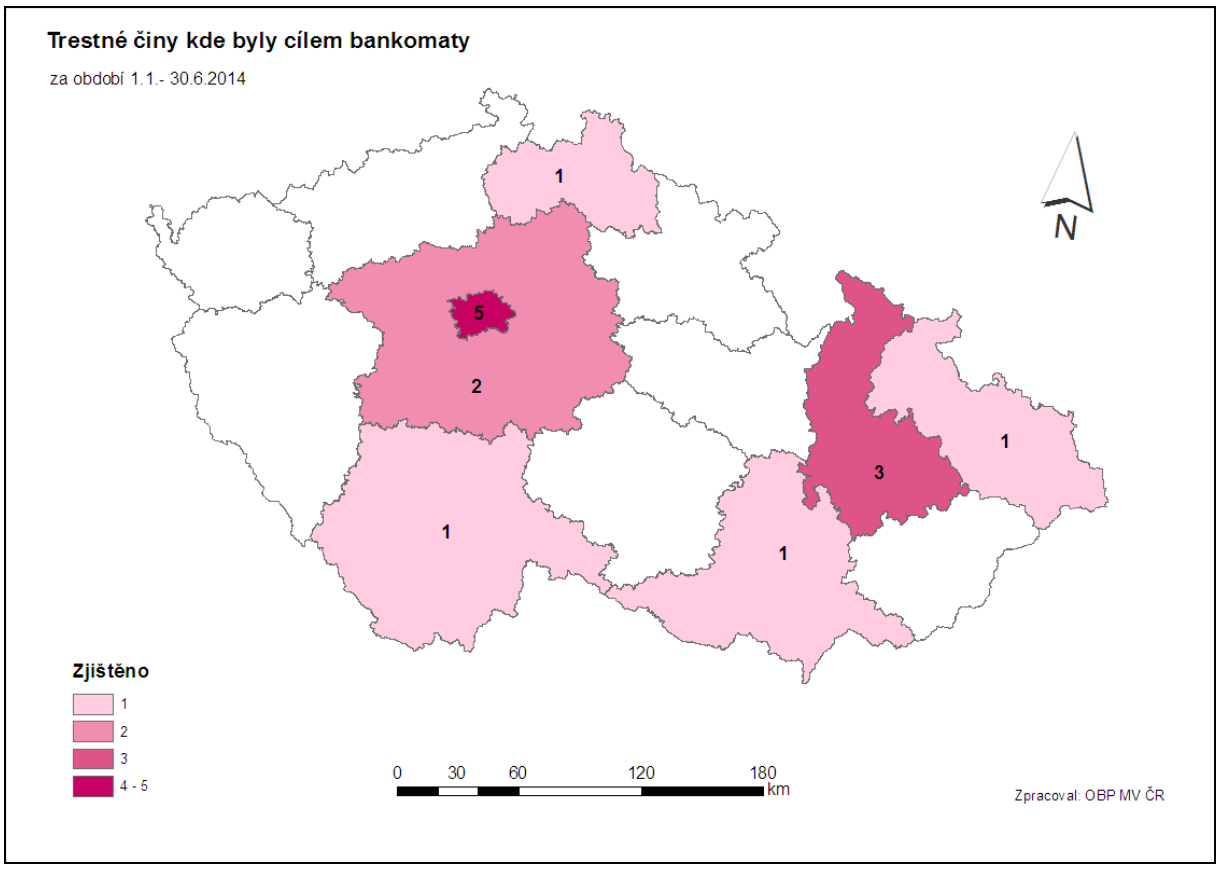
Terčem útoků se ale často stávají nejen samotné pobočky finančních institucí, ale také jejich zařízení, zejména bankomaty. V první polovině roku 2014 registrovala policie **celkem 16 případů, kde byl předmětem zájmu pachatele bankomat**. Škoda přesáhla jeden milion korun, objasněnost byla zhruba čtvrtinová (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 období leden až červen 2014

registrované skutky	16
počet skutků, u nichž byl zjištěn pachatel	4
škoda	1 125 500 Kč

Celá polovina z těchto případů byla přitom kvalifikována dle §228 jako poškození cizí věci. Skutková podstata krádeže pak byla naplněna v sedmi případech. Poslední zaznamenaný skutek byl kvalifikován jako výtržnictví.

Zřejmě největším problémem pro instituce provozující bankomaty jsou případy skimmingu, o jejichž technikách jsme již v předchozích situačních zprávách několikrát informovali. O tom, že napadání bankomatů může nabývat různých forem, svědčí nicméně kuriózní případ z května 2014. Policie v americkém Tennessee tehdy zadržela muže, který se pokoušel s bankomatem souložit. Také tento čin byl kvalifikován jako výtržnictví, lze ovšem doufat, že se v tomto případě nejedná o nový trend ohrožující bezpečnost finančních institucí.



Jak je patrné z mapy, ve sledovaném období došlo k největšímu počtu případů napadení bankomatů v Praze, 3 případy zaznamenal také Olomoucký kraj. Policie obecně v minulosti registrovali častější páchání např. skimmingu v regionech, neboť pražská policie se na tento typ trestné činnosti stále více zaměřuje.

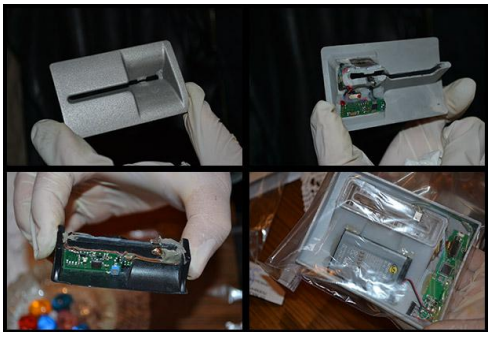
Případy skimmingu nejčastěji provádějí organizované mezinárodní skupiny. Často se na tuto činnost specializují zejména gangy ze zemí Balkánu, nejčastěji z Bulharska a Rumunska. Klíčová je v tomto ohledu především rychlá mezinárodní policejní spolupráce. Řada úspěchů byla v tomto ohledu zaznamenána na evropské úrovni. V květnu se podařilo díky spolupráci italské a bulharské policie, za asistence Europolu a Evropského centra informační kriminality (EC3), **rozbít bulharskou organizovanou skupinu, která působila v mnoha zemích Evropské unie**. Při společné akci bylo v Itálii a Bulharsku zatčeno a obviněno celkem 21 osob, nalezeno 250 zařízení pro provádění skimmingu, 2000 prázdných kreditních karet a více než 50 tisíc EUR v hotovosti.

Skupina působila téměř po celé Evropě, kde instalovala skimmovací zařízení do bankomatů. Peníze ovšem byly vybírány mimo EU – v Indonésii, USA, Bali, Dominikánské republice a v Keni. Evropské centrum EC3 během akce analyzovalo zabavená elektronická zařízení a telefonní účty. Gang se podle všeho podařilo rozbít a zadržet celý, včetně osob, které celé jednání organizovali a řídili.

Podobně úspěšnou akci zaznamenal Europol v únoru 2014 a opět se jednalo o bulharskou organizovanou skupinu. Ta se v tomto případě neomezovala jen na skimming a podvody s kreditními kartami, ale do jejího portfolia patřil také obchod s drogami, kradenými auty a příležitostná loupežná přepadení bank. V Haagu kvůli tomuto nebezpečnému gangu vznikla společná vyšetřovací skupina, která kromě expertů Europolu zahrnovala především španělské a bulharské vyšetřovatele. Po deseti měsících sběru informací v terénu proběhlo v únoru úspěšné zatčení 21 osob.

V lednu navíc Španělé zaznamenali další úspěch, když se jim podařilo odhalit jednu z největších **dílen na tisk falešných eurových a dolarových bankovek**. Španělsko-kolumbijský gang zde tiskl velmi kvalitní padělky, které byly zadrženy v hodnotě přes 100 tisíc EUR.

To, že je skimming a napadání bankomatů vysoce přeshraničním fenoménem, dokazuje ještě případ rumunské skupiny, zadržené v lednu francouzskou policií. Skupina 11 podezřelých přitom prováděla své akce převážně na italském území. Při akci bylo zadrženo také mnoho skimmovacích zařízení, přičemž dvě z nich vidíte na následujícím obrázku (vlevo). Skupina je vyráběla v malých, velmi dobře vybavených dílnách ve Francii a v Rumunsku.

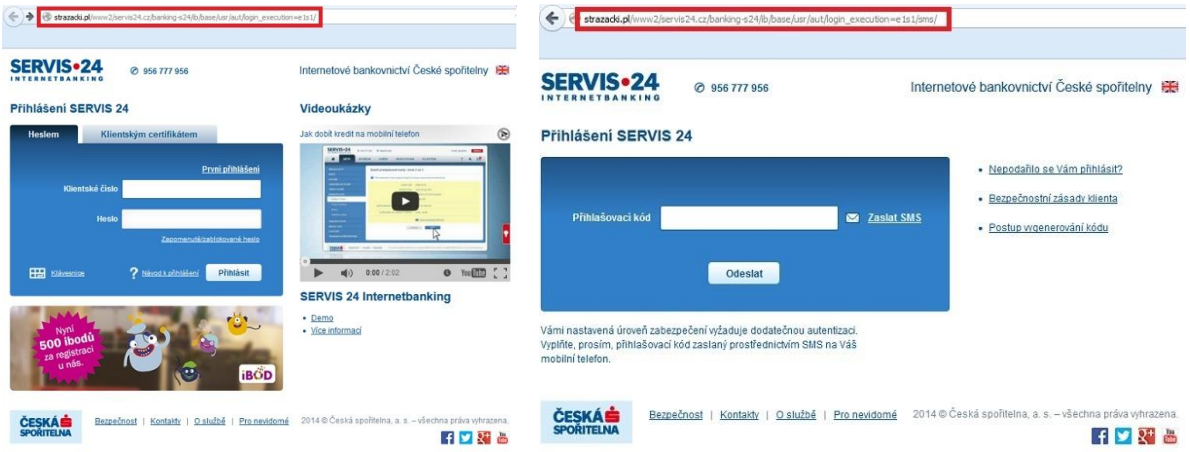


Obrázek vpravo nahoře zase ukazuje zařízení zabavené při společné akci francouzské a bulharské policie. Tato poměrně sofistikovaná zařízení pro skimming byla zadržena v květnu 2014 ve specializované dílně v bulharské Varně. Nalezeno bylo i množství mikrokamer a nástrojů pro výrobu kreditních karet. Nebyly určeny pro použití v samotném Bulharsku – mezinárodní gang je instaloval hlavně ve francouzských městech (Nancy, Mety, Lyon) a peníze vybíral na Filipínách, v Malajsii a Indonésii. Zadrženo bylo opět 11 lidí, převážně bulharské národnosti.

Lze tedy konstatovat, že i díky mezinárodní spolupráci v rámci Evropské unie se skupiny specializované na skimming kreditních karet daří úspěšně narušovat. Díky kooperaci v rámci Europolu se výrazně zlepšila efektivita a celkový přístup bulharských a rumunských bezpečnostních složek, které v roce 2014 zaznamenaly v boji s tímto fenoménem celou řadu úspěchů. Skimming je i v České republice převážně doménou občanů těchto dvou zemí EU, takže lze očekávat, že se i u nás podaří tento fenomén postupně omezovat. Techniky skimmingu a napadání bankomatů se nicméně postupně vyvíjejí, takže není zdaleka možné označit tento boj za vyhraný.

Zatímco skimming se daří pomalu, ale jistě omezovat, útoky na bankovní služby v kybernetickém prostoru mají bohužel i v ČR vzrůstající tendenci. Dle statistik společnosti Kaspersky Lab, zveřejněné v dubnu 2014, se **v České republice zvýšil v roce 2013 počet kybernetických útoků s cílem odcizit lidem peníze z bankovních účtů o 11 % na celkový počet 6250 případů**. Celosvětově byl nárůst ještě vyšší (meziročně 27,6 %; 28,4 milionů případů). Zhruba 2/3 z toho tvoří tzv. trojské koně (Zbot, Carberp, SpyEye). Časté jsou tzv. keyloggery, které se snaží zaznamenat činnost na klávesnici. Vůbec nejdramatičtější byl **nárůst tohoto typu škodlivého softwaru u mobilních zařízení** – počet malware, který se pokouší připravit uživatele o peníze, zde **vzrostl šestinásobně**.

Příkladem nebezpečného viru, cílícího na internetové bankovnictví, může být malware z června 2014. Nebezpečný odkaz přijde lidem emailem (adresa odesílatele byla původně security@ceskabank24.cz – postupně ji ale pachatelé obměňují). Vede na falešné stránky, které jsou ale mimořádně věrnou kopií portálu Servis24 od České spořitelny. Neobjevují se na nich dokonce ani žádné gramatické chyby, jako tomu bývá u jiných phishingových podvodů. Podvod tak mají šanci rozeznat jen pozorní uživatelé, kteří si všimnou nesprávného webu v adresním řádku prohlížeče. Místo servis24.cz je v něm uvedeno stazacki.pl (doménu ale pachatelé opět průběžně mění).



Pokud se na těchto podvržených stránkách přihlásíte, bude vám následně vygenerován jednorázový kód do SMS zprávy s tím, abyste ho do podvodných stránek vyplnili. Zaslaná SMS ve skutečnosti neslouží jako přihlašovací kód, ale jako ověřovací zpráva pro transakci. Právě tak se útočníci dostanou k penězům.

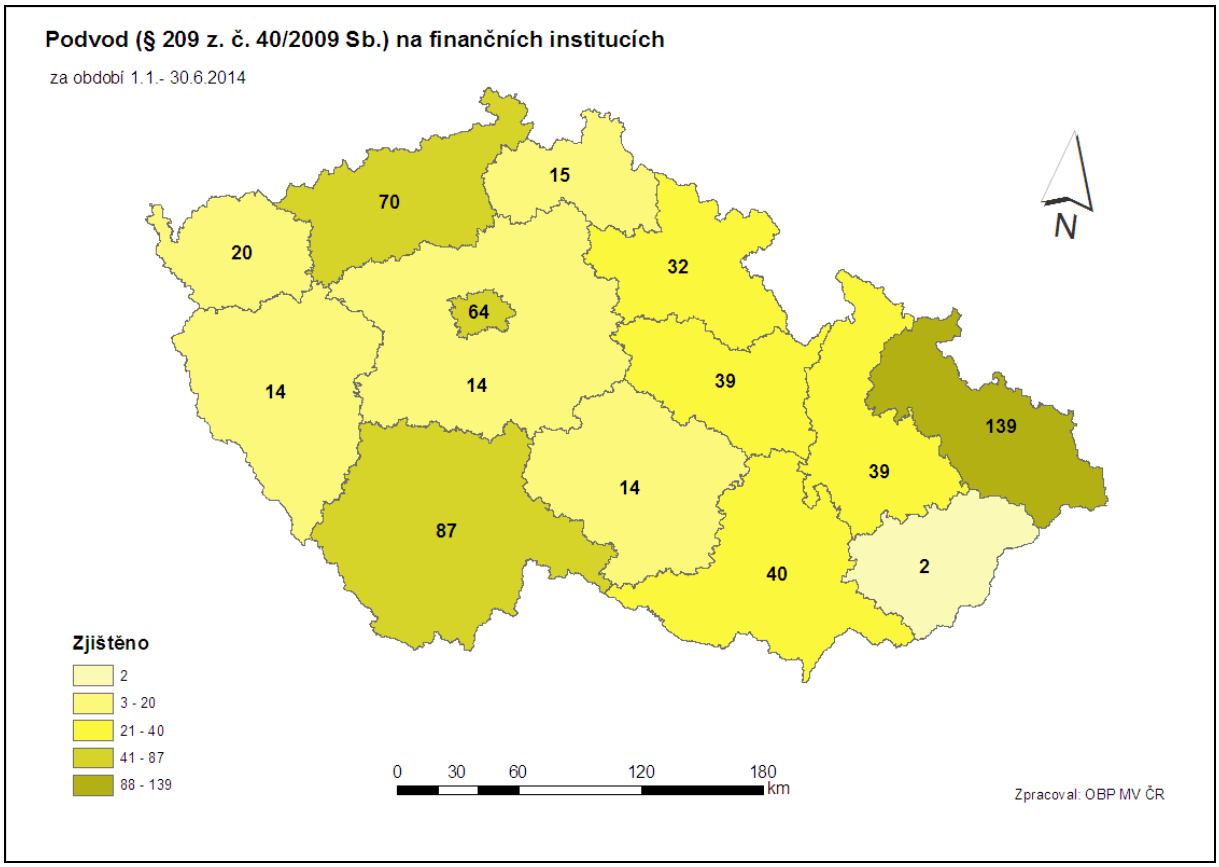
Lidé by měli obecně věnovat zvýšenou pozornost podobným zprávám, které obsahují aktivní odkazy. Pokud máte podezření, že jste takový e-mail obdrželi, neotvírejte jeho přílohy ani neklikejte na aktivní odkaz a ihned kontaktujte klientskou linku příslušné banky, případně Policii ČR např. prostřednictvím hotline pro hlášení informační kriminality na stránkách policie.cz. Některé další z mnoha případů kybernetických útoků, které letos cílili na internetové bankovnictví, zmiňujeme v kapitole věnované kybernetické bezpečnosti.

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 období leden až červen 2014

registrované skutky	585
počet skutků, u nichž byl zjištěn pachatel	337
škoda	137 351 800 Kč

Vidíme, že objasněnost se v tomto pololetí pohybovala na 57 %. Co se týče geografického rozložení, pak se v tomto případě jedná o jeden z mála trestných činů, ve kterém nevévodí Praha. Ta je s 64 spáchanými skutky dokonce až na čtvrtém místě a překonávají ji kraje Moravskoslezský (139 případů), Jihočeský (87 případů) a Ústecký (70 případů).

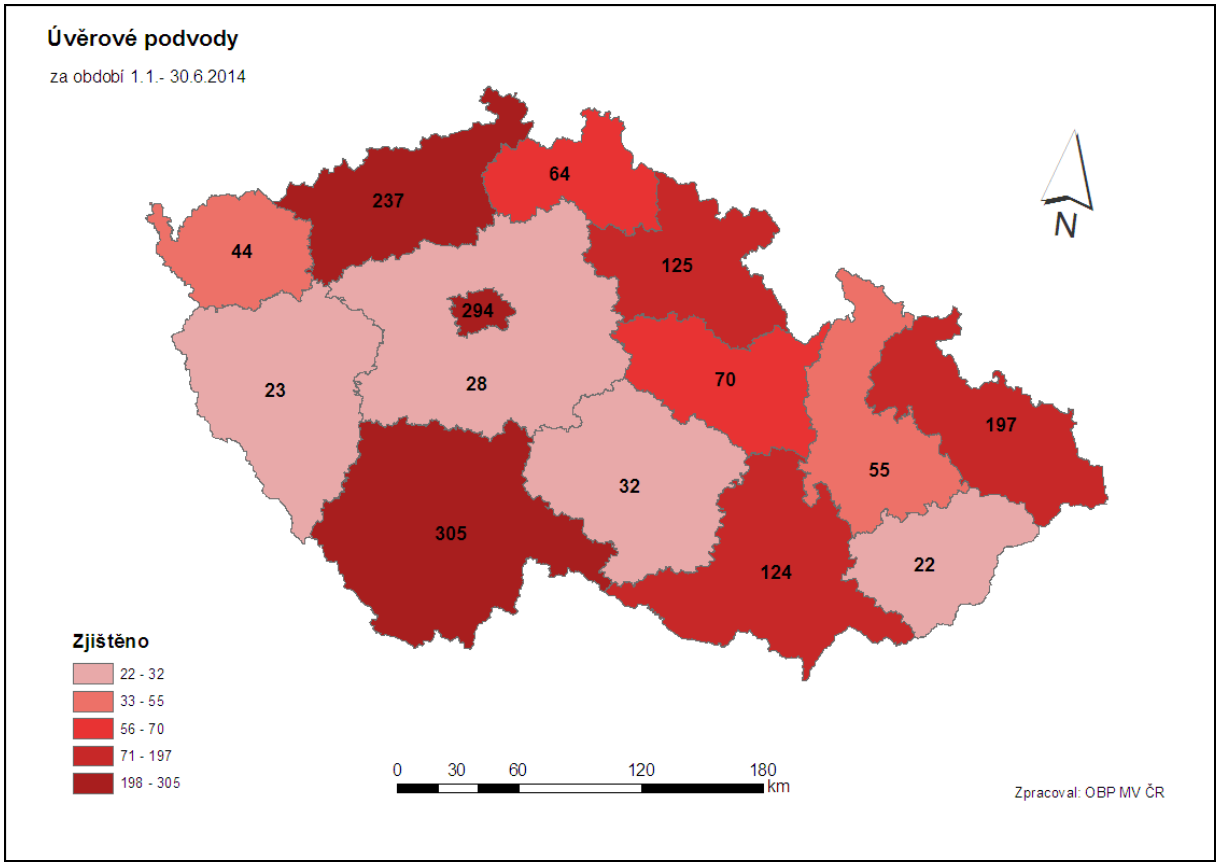


Pokud se dále zaměříme na problematiku **úvěrového podvodu** (§211), získáme následující čísla:

úvěrový podvod (§ 211 z. č. 40/2009 Sb.) na finančních institucích
objekt hospodářské kriminality za období leden až prosinec 2013

registrované skutky	1 620
počet skutků, u nichž byl zjištěn pachatel	1 121
škoda	386 203 700 Kč

Objasněnost úvěrových podvodů je značně vysoká, v 1. pololetí roku 2014 se pohybovala zhruba na 70 %. V roce 2013 byla policie ještě úspěšnější a rozkryla celých 84 % úvěrových podvodů.



Fenomén: rizika virtuálních měn

Virtuální měny se postupně stávají často využívanou alternativou státem garantovaných platebních systémů. V případě, že všichni účastníci směny uznávají jejich hodnotu, mohou fungovat do značné míry stejně jako běžné národní měny, ačkoliv většina států je za skutečnou „měnu“ neuznává. Například americká vláda nepovažuje virtuální platidla za měny, ale za nehmotný majetek, který tudíž podléhá zdanění (precedentní rozhodnutí texaského soudu ale jednu z virtuálních měn za peníze označilo). Naopak v Dánsku jsou virtuální měny sice rovněž považovány za „zboží“ (a nikoliv platidlo), ale daně se na ně nevztahují. Německé ministerstvo financí se zase vyjádřilo v tom smyslu, že platební systém Bitcoin považuje za soukromé peníze, čímž mu de facto status měny přiznalo.

Právě Bitcoin, který vznikl v roce 2009, je zřejmě celosvětově nejznámější virtuální měnou, třebaže existuje řada dalších. Tato analýza se pokouší pojmenovat některá nejčastější rizika, spojená s virtuálními platidly. Vzhledem k jeho největší rozšířenosti bude často zaměřena právě na Bitcoin.

Nejistá investice

Hlavní výhodou virtuálních měn je pro některé uživatele fakt, že tato platidla jsou anonymnější a nezávislejší tj. méně podléhají vlivům a regulacím centrálních bank a vlád. Méně se jich tak dotýkají např. hospodářské problémy jednotlivých států, ekonomické sankce, monetární a fiskální politiky jednotlivých zemí atd.

To ovšem zároveň znamená, že jejich hodnota není v reálném světě ničím podložena ani garantována (např. státním majetkem). Ačkoliv je již dávno pryč doba, kdy byly všechny národní měny reálně kryty zlatem a prakticky veškerá platidla jsou dnes založena především na důvěře jejich uživatelů, u virtuálních měn to platí dvojnásob. Jejich kurz tedy často výrazně kolísá a v případě ztráty důvěry mohou (daleko snáze než národní platidla) velmi rychle ztratit hodnotu či zcela zaniknout. Investice do těchto měn proto sice může slibovat vysoké zisky, na druhou stranu je ale také velmi riziková.

Dobře to dokládá vývoj kurzu výše uvedené virtuální měny Bitcoin. Bitcoin je v podstatě speciální software, který umožňuje jeho uživateli nakládat a obchodovat s těmi prostředky, které zakoupil, či si je „vytěžil“. Celkový počet bitcoinů v oběhu je totiž předem daný, aby se zabránilo inflaci uměle vytvořené jeho navyšováním. Bitcoinů má být celkem zhruba 21 milionů, přičemž jsou do oběhu vypouštěny postupně prostřednictvím tzv. „těžby“ – každý uživatel softwaru má možnost věnovat část operační kapacity svého počítače k tomu, aby nové bitcoiny vytvářel. Tato těžba se postupně zpomaluje (uživatelé, kteří začali „těžit“ v počátcích projektu, si za stejný čas přišli na mnohem větší počet bitcoinů, než ti později

příchozí), přičemž odhadem v roce 2140 se těžba zastaví úplně (reálně bude ale většina bitcoinů vytěžena již kolem roku 2030). Těžba je tím úspěšnější, čím výkonnější počítač uživatel používá, přičemž „těžaři“ se často sdružují do skupin. Nakolik je tato činnost rozšířená, svědčí fakt, že při těžbě bitcoinů se odhadem denně ve světě spotřebuje elektřina v hodnotě až 300 milionů Kč.

Cena Bitcoinu začala krátce po jeho zpopularizování raketově růst. Na těžbě bitcoinů tak bylo teoreticky možné v počátcích velmi rychle zbohatnout, neboť jejich hodnota se během jednoho roku zmnohonásobila. Po roce 2012 ale začala měna procházet krizí důvěry a její hodnota začala velmi dramaticky kolísat. Například zatímco v listopadu 2013 se pohybovala na hodnotě 1250 dolarů, o měsíc později se kvůli restrikcím v Číně propadla na 421 dolarů, jen aby lednu 2014 opět její hodnota přesáhla 1000 dolarů.

Velkou ránu způsobil důvěře v toto platidlo pád velké kybernetické burzy Mt. Gox, kde bylo možné tuto virtuální měnu směňovat za měny „skutečné“. Z této burzy se neznámým způsobem v únoru 2014 ztratilo 740 000 bitcoinů. Japonské i americké úřady vyšetřují, zda byla tato obrovská částka (podle tehdejšího kurzu v řádu miliard korun) ukradena či zpronevěřena, jejich majitelům se ale podle všeho peníze už nikdy nevrátí. Tato událost silně otřásla důvěrou v celou virtuální měnu, tím spíše, že již v březnu 2014 se stala terčem úspěšného hackerského útoku banka Flexcoin, která přišla o bitcoiny v hodnotě zhruba 600 000 dolarů a vzápětí zkrachovala.

Ještě před těmito událostmi varoval před riziky bitcoinů a dalších virtuálních měn Evropský bankovní úřad (EBA). Ten v prosinci 2013 uživatele systému upozornil, že se na něj nevztahuje pojištění, které v EU platí pro běžné bankovní vklady a v případě hackerského útoku či neúspěšného transferu peněz tak (na rozdíl od běžných bankovních transakcí) nelze spoléhat na žádnou institucionální ochranu či žádat odškodné. Nezávislost na úřadech pro uživatele virtuálních měn tedy zároveň znamená, že se nemohou u úřadů domáhat náhrady škod za případnou újmu. Investice např. do bitcoinů je tak soukromým rizikem každého jednotlivce.

Zneužití virtuálních měn ke kriminálním aktivitám

Pro řadu zločinců a kriminálních organizací byl zrod virtuálních platidel doslova darem z nebes. Ačkoliv jejich vznik zřejmě nebyl přímo motivován pomocí kriminálníkům, charakter těchto prostředků v podstatě přesně vyhovoval jejich poptávce po anonymní a obtížně vysledovatelné možnosti převodu peněz jak v rámci jednotlivých států, tak především mezinárodně.

Z tohoto důvodu se např. bitcoin stal běžně využívaným prostředkem pro činnost překupníků drog, ilegálních obchodníků se zbraněmi, teroristů a hackerů. Pro policii a bezpečnostní složky se naopak jedná o výraznou překážku, neboť jednou z nejčastějších vyšetřovacích metod při rozkrývání mezinárodního organizovaného zločinu bylo sledování finančních toků. Používání virtuální měn v kombinaci s anonymizačním softwarem sledování finančních transakcí výrazně ztěžuje a v některých případech zcela znemožňuje, neboť probíhá mimo zavedené bankovní a finanční instituce a de facto zcela mimo „běžný“ peněžní systém. Zločinci a teroristé si tak mohou vyměňovat prostředky velkou rychlostí na neomezenou vzdálenost s mnohem nižším rizikem dopadení.

Právě s rozšířením bitcoinů je spjat vznik a rozvoj skrytých internetových tržišť, na kterých se často nabízejí ilegální zboží a služby. Zřejmě nejznámějším takovým portálem byl americký

Silk Road (Hedvábná stezka) uzavřený koncem září 2013. V roce 2012 na něm probíhaly obchody tisíců prodejců, přičemž celkový obrat se odhadoval na desítky milionů dolarů ročně. Hedvábná stezka se brzy stala jakýmsi virtuálním centrem prodeje drog, nabízel se zde hlavně kokain a heroin ve velkých i malých objemech. Výjimkou ale nebyly ani nabídky ilegálních zbraní, údajně se objevily dokonce poptávky po nájemných vraždách.

Silk Road umožňoval prodejcům i nakupujícím přísnou anonymitu díky používání systému Tor, maskujícího IP adresy. Podle amerických policistů se přes něj ročně prodalo několik set kilogramů narkotik. Zboží se většinou doručovalo běžnou poštou, nebo prostřednictvím kurýrních služeb na adresu uvedenou kupujícím. Obvykle šlo o zásilku ve vakuovém balení, které znesnadňuje odhalení jejího obsahu čichacími psy. Zásilka byla často maskována obálkami s hlavičkou reálných nebo fiktivních firem. Nabídku k zakoupení kvalitního heroinu či kokainu využívali údajně i čeští uživatelé.

Platilo se přitom právě výhradně těžko vystopovatelnou virtuální měnou Bitcoin, pro kterou v té době v podstatě neexistovala žádná právní úprava. Dealer drog a jeho zákazník tak mohli být od sebe vzdáleni tisíce kilometrů a jeden druhého nemusel vůbec nikdy vidět. Celý systém fungoval na důvěře a propracovaném systému referencí od „spokojených zákazníků“. Třebaže se na Silk Road nabízelo i legální zboží, objem ilegálních aktivit postupně výrazně převládl.

Americkým úřadům nakonec došla trpělivost a tvůrce webu, devětadvacetiletý William Ulbricht ze San Francisca, byl v říjnu 2013 FBI zatřen. Zároveň byla při zásahu zabavena virtuální měna bitcoin v hodnotě 3,6 milionu dolarů (asi 68 milionů korun). Ulbricht byl obviněn ze spiknutí k obchodování s drogami, hackerství a ze spiknutí k praní špinavých peněz. Prozradila ho přitom poměrně triviální chyba, kdy se na odborných technických stránkách ptal vlastním jménem na specifický kód pro skryté internetové stránky, který později použil právě při tvorbě Hedvábné stezky.

Na základě podobných stop byl v nedávné době některými uživateli internetu podezírán český občan z vytvoření a následného „vytunelování“ online tržiště Sheep Marketplace, které bylo označováno za nástupce Silk Road. Toto internetové tržiště přerušilo na přelomu listopadu a prosince 2013 nečekaně svůj provoz. Jeho administrátoři nejprve zveřejnili zprávu o tom, že se portál stal terčem hackerského útoku, následně ho ale bez varování uzavřeli a zcela přestali komunikovat. V jejich držení tak podle časopisu Forbes zřejmě zůstává zhruba 40 milionů dolarů (800 milionů korun) ve virtuální měně Bitcoin. Podle některých zdrojů mohlo být Sheep Marketplace řízeno z České republiky, identita jeho tvůrců ale zůstává nejasná.

Některé stopy vedly k českému programátorovi, který před časem na českých i zahraničních fórech hledal rady ohledně provozování skrytého online tržiště. Ten ale své zapojení do projektu důrazně odmítá, bránit se hodlá i právní cestou. Vypátrali ho sami uživatelé internetu, a to podobným způsobem, jakým byl odhalen Ulbricht (dotazy na internetových fórech), přičemž někteří z nich po něm již požadují navrácení ukradených peněz, a dokonce mu vyhrožují fyzickou likvidací (mezi obětmi podvodu je pochopitelně řada zločinců, zejména z řad distributorů drog).

V současné době se přitom hovoří o tom, že tržiště Silk Road bylo v nové podobě opět obnoveno. Je velmi pravděpodobné, že vznik podobných platforem byl přímo podmíněn vznikem těžko vysledovatelných virtuálních měn. Podobné ilegální obchody se přitom zdaleka nemusejí odehrávat jen na internetových tržištích, stejně dobře mohou posloužit diskusní fóra. Placení s pomocí bitcoinů bývá také využíváno pro financování terorismu.

Využívat je mohou i vyděrači – v minulé situační zprávě jsme v sekci věnované kybernetické bezpečnosti informovali o novém úspěšném počítačovém viru Cryptolocker, který data na napadeném zařízení zašifruje prakticky neprolomitelným kódem a za jejich odblokování požaduje výkupné. Není jistě náhodou, že toto výkupné má oběť útoku zaplatit právě v nevystopovatelných bitcoinech.

Jiné, nově se šířící počítačové viry, se zase snaží zneužít kapacitu Vašeho počítače k „těžbě“ bitcoinů. Ta běží na pozadí, aniž by ji uživatel spustil nebo ji mohl zastavit a výrazně zpomaluje chod zařízení. Je přitom zřejmé, že „vytěžené“ bitcoiny z tisíců takto napadených počítačů využívají tvůrci malware. Velmi běžné jsou i hackerské útoky, mající za cíl krádež bitcoinů. V prosinci 2013 zase německá policie zadržela muže, kteří jsou podezřelí za padělání bitcoinů v hodnotě 19 milionů Kč.

Regulace virtuálních měn a jejich rozšíření v ČR

Široké zneužívání virtuálních platidel zločinci vedlo některé státy k úvahám o jejich regulaci a začlenění do běžného právního rámce, ze kterého se doposud vymykaly. Americký Senát již v srpnu 2013 projednával opatření, která by mohla bránit ve využívání virtuálních měn ke kriminálním aktivitám. Vyšetřovatel newyorského oddělení úřadu pro regulaci finančních služeb Benjamin Lawsky označil virtuální měny za "divoký západ" pro zločince.

Bitcoin chtějí kvůli jeho zneužívání pro praní špinavých peněz regulovat i Rusové. Ruská centrální banka koncem června 2014 oznámila, že se připravuje legislativa pro jeho regulaci. Někde se naopak uvažuje o začlenění bitcoinů a dalších virtuálních měn do běžného finančního systému, přičemž by s ním mohly obchodovat také banky a finanční instituce.

Bitcoiny jsou přitom stále populárnější také v České republice. Od května 2014 má i Praha svůj první bitcoinový bankomat. Těch v té době ve světě existovalo sotva dvacet. V červenci 2014 navíc začala fungovat jeho první česká alternativa – virtuální měna Czech Crown Coin, které mělo být vydáno celkem asi 100 milionů mincí. Polovina z tohoto počtu je již předtěžena, zbytek bude vydáván následujících zhruba 10 let. Stránky projektu byly však již v první den existence nového českého virtuálního platidla napadeny DDoS útokem, což důvěru případných klientů v nový systém příliš neposílilo.

Vybrané události ve sledovaném období

Leden

Poslední loni vyloupená pražská banka byla letos vyloupena jako první
První letošní pražská bankovní loupež se odehrála v pobočce peněžního domu v Táboritské ulici. Tatáž banka byla poslední vyloupenou bankou v roce loňském. Do bankovní pobočky vešel muž se stříbrnou pistolí v ruce. Po pokladní okamžitě požadoval vydání veškeré finanční hotovosti, načež obdržel několik desítek tisíc korun. Poté utekl neznámo kam.
Banka v Táboritské ulici bohužel patří mezi ty pobočky, které si lupiči vyhlédli již několikrát. V roce 2009 se stala např. terčem „rychlolupiče“, který v Praze přepadl tři banky v průběhu pouhých patnácti minut a odnesl si celkem přes milion korun. Dva měsíce od jeho první akce jej ale dopadli policisté a skončil ve vězení.

Nejpadělanější desetieurová bankovka dostala nové ochranné prvky

Evropská centrální banka představila novou desetieurovou bankovku. Jedná se o druhý produkt z nové série platidel s posílenou ochranou před padělaním. Na nové desetieurovce se objeví obraz bájné řecké princezny Europy.
Nová desetieurovka bude teprve druhou bankovkou eura, která se dočká výraznějších změn. Jako první to byla nejpoužívanější pětieurová bankovka, kterou šéf ECB Mario Draghi představil před rokem a v oběhu je od května. Na ní se Europa v podobě vodoznaku a hologramu objevila poprvé. Evropské bankovky mají více bezpečnostních prvků a díky speciálnímu laku získávají i nový, odolnější nátěr. Po desetieurové bankovce má přijít příští rok do oběhu bankovka v hodnotě 20 eur.

Únor

Dvojice chtěla vykrást bankomat, použila k tomu výbušninu
Dvojice mužů chtěla na pražské Skalce vykrást bankomat České Spořitelny, ke svému činu použila doposud neznámou výbušninu. Následných výbuch rozbil skleněnou výlohu a poškodil majetek České Spořitelny. Škoda byla odhadnuta na 600 tisíc korun, avšak žádné peníze se dvojici z bankomatu nepodařilo odcizit. Následně z místa oba muži utekli. Do Vyžlovské ulice následně zamířily hlídky PČR, policejní pyrotechnik a chemici HZSPraha ze stanice Petřiny. Výbuch naštěstí nikoho nezranil.

Za sex platil muž v Ostravě padělanými bankovkami
Kriminalisté odboru hospodářské kriminality začali v květnu minulého roku prověřovat informace k tehdy neznámému muži, který měl s největší pravděpodobností platit padělkem bankovky v hodnotě 2 000 korun. Bankovku policistům vydala mladá žena. Sdělila jim, že se s neznámým poznala prostřednictvím internetové seznamky. Domluvili si v Ostravě společnou schůzku za účelem sexuálních služeb. Smluvené proběhlo a muž jí zaplatil. Když chtěla žena následně platit dvoutisícikorunou za zboží v obchodě, prodavačka jí sdělila, že se jedná zřejmě o padělek. Kriminalisté zajištěnou bankovku zaslali České národní bance k odbornému vyjádření. Z výsledku vyplývá, že se jedná opravdu o padělek.Kriminalisté od samotného počátku prověřovali vše, co by je mohlo dovést na stopu pachatele. Kromě detailního zadokumentování informací od mladé žen také zjistili, že stejný modus operandi vykazovalo jednání z léta minulého roku v Olomouci – platba padělkem dvoutisícikoruny za sexuální služby.

Olomoučtí kolegové již znali totožnost muže a porovnáním obou případů bylo prokázáno, že se jedná o téhož pachatele. Kriminalisté jeho vytěžením zjistili, že měl v polovině minulé roku doma vyrobit na běžném zařízení bankovky různých hodnot. Jelikož se mu například dvousetkoruny nepovedly, vyhodil je do koše. Bankovky v hodnotě 2 000 korun se mu zdály dobré, tak si jich několik dal do peněženky. Původní úmysl platit padělky třeba za benzin si rozmyslel z obav pečlivé kontroly peněz obsluhou. A druhou variantou bylo ušetřit tak při placení za sexuální služby. Nyní je obviněn ze zločinu padělání a pozměnění peněz.

Březen

Jihočeští kriminalisté dopadli mimořádně nebezpečné padělatele

Jihočeští kriminalisté obvinili dvojici mužů z Bulharska ze zločinu padělání a pozměnění peněz, zadržení udávali padělané 200 eurové bankovky mimořádně nebezpečné kvality.
Jihočestí kriminalisté se zaměřili na možné padělatele eurových bankovek, v nominální hodnotě 200 Eur. Ty se totiž začaly vyskytovat od loňského léta po celém kraji a také na dalších místech republiky. Všechny zjištěné informace je nakonec dovedli k dvojici možných pachatelů, kteří se po republice pohybovali se dvěma vozidly Fordem Fiesta černé barvy a Mazdou 121, obě vozidla byla opatřena bulharskými registračními značkami. Kriminalisté vyhlásili po dvojici mužů z Bulharska (56 let a 49 let) celostátní pátrání a to s ohledem na jejich pohyb po celé republice. Postup se osvědčil a muže zadrželi dopravní policisté z Kladna. Jihočeští kriminalisté si oba zadržené včetně vozidla eskortovali do Českých Budějovic.
Muže obvinili ze dvou závažných skutků, a to ze zločinu padělání a pozměňování peněz a z podvodu. Kriminalisté zatím dvojici prokázali více jak desítku padělaných eurových bankovek v nominální hodnotě 200 Eur. Česká národní banka zajištěné padělky ohodnotila druhým nejvyšším stupněm nebezpečnosti. Padělky jsou totiž opatřeny téměř všemi ochrannými prvky.
Například napodobený hologram je velmi zdařilý, pod UV světlem se dokonce objevují i některé správné prvky. Podle dokonalosti padělku je běžný obchodník nedokáže rozpoznat. Padělané bankovky odhalili až pracovníci bankovních ústavů.
Oba dva obvinění udávali padělané bankovky v barech, na čerpacích stanicích a obchodech, udělali drobný nákup a zaplatili padělanou dvou set eurovou bankovkou nebo požadovali rozměnit. Muži se snažili při nákupech hovořit německy.

Bankovky na letišti v Ruzyni vyčenichá služební pes

Ruzyňští celníci začali využívat další účinný prostředek na kontroly převozu finanční hotovosti, služebního psa. Celní správa České republiky se tak zařadila do skupiny členských států Evropské unie, které aktivně bojují s „praním špinavých peněz" s pomocí speciálně vycvičených psů. Ty ke kontrolám tohoto typu využívají například Celní správy Spolkové republiky Německo, Nizozemska, Rakouska či Itálie.
Během svého krátkého působení se podílela fenka belgického ovčáka jménem „Boxy" na odhalení devíti případů nelegální přepravy finanční hotovosti. Celkem bylo zajištěno 112 870 EUR a 61 400 USD, což je v přepočtu více než 4 340 000 korun. Kontroly jsou prováděny na základě platné legislativy Evropské unie a zákona „o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu". Pokud cestující vstupuje na území EU nebo naopak z tohoto území vystupuje má povinnost písemně oznámit celnímu úřadu na předepsaném tiskopisu dovoz a vývoz platných platidel v české nebo cizí měně, v úhrnné hodnotě převyšující 10 000 EUR. Pokud cestující tuto povinnost nesplní, hrozí mu sankce pokuty až do 10 miliónů korun nebo propadnutí věci.

Policie dopadla lupiče z pražské Koněvovy ulice
Kriminalisté z Prahy zadrželi trojici mužů, kteří podle policie počátkem loňského února poblíž pražské Koněvovy ulice ukradli ze zaparkované dodávky bezpečnostní agentury téměř 18,5 milionu korun. Jeden z nich tehdy v agentuře pracoval. Zaměstnanec bezpečnostní agentury se podle policie dohodl se svými komplici, že dodávku odstaví na domluveném místě za poštovním úřadem. Zbylí dva muži rozlomili zámek dveří a odcizili hotovost. Policie muže ve věku 34, 43 a 53 let obvinila z krádeže a poškození cizí věci, hrozí jim až deset let vězení. Soud je poslal do vazby.
Na místě krádeže se podařilo zajistit minimum upotřebitelných stop, chyběli i svědci nebo záběry z městského kamerového systému. I tak kriminalisté trojici po několika měsících začali podezřívat, neměli ale dostatek důkazů. Nakonec proti pachatelům svědčila, krom jiného, především jejich vlastní chamtivost. Muži splatili dluhy, přestěhovali se do nemovitostí s vysokým nájmem a koupili si luxusní auta.
Muže podezřelé z krádeže zatkla pražská zásahová jednotka, protože se předpokládalo, že některý z nich může být ozbrojen. To se nakonec i potvrdilo, když u jednoho ze zadržovaných policisté zajistili nelegálně drženou pistoli ráže devět milimetrů s vypilovaným číslem.

V bance na Václavském náměstí nechal lupič funkční bombu, pyrotechnici ji zneškodnili
Bankovní pobočku ČSOB na Václavském náměstí v centru Prahy se pokusil vyloupit muž. Policisté dostali oznámení o přepadení banky - do jednoho z bankovních domů na Václavském náměstí přišel muž s koženým kufrem, bankovní úřednici položil kufr na stůl a sdělil jí, že požaduje vydání větší finanční hotovosti a že v kufru má výbušninu. Úřednice prý lupiči řekla, že tolik peněz u sebe nemá, muž pak odešel.
V kufříku, který muž po neúspěšném pokusu o loupež zanechal v bance na Václavském náměstí v Praze, byl podle policie nástražný výbušný systém. Podle pyrotechniků byla bomba funkční.

Duben

Policisté dopadli muže, kvůli kterému v Příbrami evakuovali 8 bank
Obvinění z přečinu šíření poplašné zprávy si vyslechl 37letý muž z Příbramska, měl zavolat z mobilního telefonu na tísňovou linku 112, kde úmyslně oznámil nepravdivou informaci o tom, že se v jedné z příbramských bank nachází bomba.
Kvůli této zprávě bylo uzavřeno, vyklizeno a evakuováno celkem osm bank. Policisté a psovodi se psy specializujícími se na vyhledávání výbušnin prohledali prostory uzavřených objektů. Žádná bomba však nalezena nebyla. Vzniklá škoda zatím nebyla přesně stanovena. Obviněný muž rozšířil poplašnou zprávu, která mohla vyvolat vážné znepokojení části obyvatelstva, a také z tohoto důvodu došlo k bezdůvodné práci integrovaného záchranného systému. Důvodem jeho činu mohlo být to, že měl vrátit známému dlužnou částku, kterou s ním šel právě v inkriminovanou dobu vybrat do banky, ale zřejmě mu peníze dát nechtěl. Těsně před výběrem došlo k uzavření objektu z důvodu nahlášené výbušniny.

Realitní makléř s dětskou pistolkou vyloupil čtyři banky

Až deset let za mřížemi hrozí realitnímu makléři, postupně podle vyšetřovatelů přepadl čtyři banky a odnesl si 1,3 miliónu korun. Devětadvacetiletý muž měl podle spisu nejprve navštívit prodejnu žertovných předmětů v Praze. Zde nakoupil upírské zuby a chrup zombie, rukavice s kostlivcem a žertovné brýle. V přestrojení pak podle vyšetřovatelů od února 2009 do srpna 2013 vyloupil banky v Třebíči a Praze. Na tvář si přitom měl ještě nanést silnou vrstvu make-upu, k tomu si dle spisu narazil paruku, oblékl se do většího oděvu a na nohy obul o několik čísel menší boty, což mělo znesnadnit pátrání. Po svém zadržení přiznal, že byl ve finanční tísni. Případem se začal zabývat brněnský Krajský soud, který obžalovanému muži prodloužil vazbu.

Květen

Muž v Praze přepadl banku, zadrželi ho policisté z SPJ Praha

V ulici Na Slupi v Praze došlo k loupežnému přepadení tamní bankovní pobočky. Do té pár přišel neznámý muž a namířil přímo k pokladní přepážce, kde úřednici předložil lístek s požadavkem k vydání finanční hotovosti. Jelikož úřednice neviděla v rukou pachatele žádnou zbraň, tak se obě ženy se před lupičem schovaly a uzamkly v jedné z místností banky. Ve chvíli, kdy zůstal za přepážkami lupič osamocen, této chvíle využil a přisvojil si veškeré nalezené bankovky. S těmi pak chtěl odejít z pobočky pryč. V tu chvíli ale k bance už přijížděly první policejní hlídky, před kterými se lupič schoval v jedné z místností pobočky, kde se i uzamkl.
Na místo také přijelo družstvo Speciální pořádkové jednotky, jejíž policisté následně provedli zákrok. Ti za pomoci technických prostředků otevřeli uzamčené dveře a zadrželi jedenatřicetiletého pachatele. Toho následně převezli na policejní služebnu k provedení úkonů trestního řízení.

Policisté varují před e-maily s výzvou k zaplacení dlužné částky

Policisté se zabývají novými případy podvodných e- mailů s výzvou k zaplacení dlužné částky. Celorepublikově už se jedná o stovky případů. Na policisty se obrátilo několik poškozených, kterým do jejich e-mailové schránky přišla výzva k zaplacení dlužné částky v řádu několika tisíců korun. Kromě výzvy k uhrazení dluhu je v příloze e–mailu také soubor zip, který je označen jako smlouva a její číslo. Po otevření tohoto souboru se do počítače uživatele dostane vir, který odesílateli podvodné zprávy umožní neoprávněný přístup do systému a získání dat.

Červen

Policisté dopadli anonymního volajícího, který oznamoval bombu

Policisté dopadli muže, který dvakrát anonymně zavolal na linku 112, že ve spořitelně ve Valašském Meziříčí je bomba. Důvodem jeho počínání bylo zabránit jeho matce dostat se do spořitelny, kde by zjistila, že jí neoprávněně vybral z účtu několik desítek tisíc korun.
Na místo vyjeli neprodleně valašskomeziříčtí policisté společně se strážníky městské policie, kteří nejprve evakuovali 13 zaměstnanců a 17 zákazníků, a následně celý objekt důkladně prohledali. Žádný nástražný výbušný systém nenašli a pobočka spořitelny tak mohla být před třetí hodinou pro zákazníky otevřena. Totéž se odehrálo i o pár dní dříve.
Valašskomeziříčským policistům se podařilo chvíli po anonymním telefonátu zjistit, kdo hovory uskutečňoval. Šiřitelem poplašných zpráv byl šestadvacetiletý mladík z Valašského Meziříčí. Dluhy ho přiměly k tomu, že vzal své matce platební kartu, prostřednictvím které z jejího účtu postupně vybral několik desítek tisíc korun. Kartu pak poškodil, aby nebyla použitelná. Když matka mladíka poškození karty zjistila, chtěla jít tuto záležitost do spořitelny řešit.
Matka se po skončení policejní prohlídky do spořitelny dostala a neoprávněný výběr zjistila. Z peněžního ústavu šla rovnou na policii neoprávněné výběry oznámit. Podezření padlo na syna matky, který se při výslechu nakonec policistům přiznal. Policisté sdělili mladíkovi podezření ze dvou trestných činů: šíření poplašné zprávy a neoprávněné opatření, padělání a pozměnění platebního prostředku.

Národní bezpečnostní tým varuje před útoky na internetové bankovnictví

Národní bezpečnostní tým CSIRT.CZ vydal varování před podvodníky, kteří se snaží ukrást přihlašovací údaje k internetovému bankovnictví. Podobné varování o pár dní dříve vydalo i Sdružení pro bankovní karty. Uživatelé by si také neměli všímat nabídky lukrativní pracovní pozice ve finančním sektoru.

Nové útoky na internetové bankovnictví se pokoušejí nachytat uživatele tzv. phishingem. Národní bezpečnostní tým tak varuje před e-mailovou zprávou, která se snaží uživatele internetového bankovnictví ČSOB donutit či nalákat ke kliknutí na odkaz, který e-mail obsahuje. Pokud to uživatel udělá, bude přesměrován právě na phishingovou stránku, kde se může nacházet například kopie přihlašovací stránky k internetovému bankovnictví. CSIRT.CZ již požádal o odstranění phishingových stránek u příslušných administrátorů. Samotná e-mailová zpráva je naštěstí velmi primitivní. I zákazníci jiných bank než ČSOB by se měli mít na pozoru. Vlastní varování totiž vydalo Sdružení pro bankovní karty. Podle něj se nyní Česko potýká dokonce s celou vlnou nových phisingových útoků.

Pachatel stihl po přepadení utratit 350 000 Kč, i když jej policie zadržela druhý den

Muž se před přepadením potuloval centrem Brna a v kapse měl lístek s výhružným nápisem, že má u sebe granát. Když se ochomýtal kolem jedné z poboček, napadlo ho, že by mohl svůj plán uskutečnit. Vzal proto za kliku, ale banka byla ještě zavřená. Muž se proto šel do nedalekého obchodu, kde si dal zmrzlinu, aby si zkrátil čekání.

Hned po otevření zamířil k jedné z přepážek a pracovnici předložil lístek. Požadoval vydání půl miliónu korun. Žena začala pokládat bankovky na pult a mezitím stiskla tlačítko alarmu, aby upozornila ostrahu objektu. Muž znervózněl a řekl, že už je peněz dost, a z místa utekl. Odnesl si více než tři sta padesát tisíc korun. Peníze ihned utratil, kriminalisté mu ale byli rychle na stopě a druhý den po přepadení ho zadrželi v jednom z brněnských penziónů.

Vyšetřováním pak zjistili, že lupič má na svědomí i výhružku bombou, neboť na začátku června zavolal na linku 158 s tím, že v jednom z domů v Tišnově je uložena výbušnina a za třicet minut vybuchne. Policisté tehdy museli evakuovat 40 lidí.

Zdroje pro tuto kapitolu: policie.cz, 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,

INFORMAČNÍ TECHNOLOGIE A KYBERNETICKÁ BEZPEČNOST

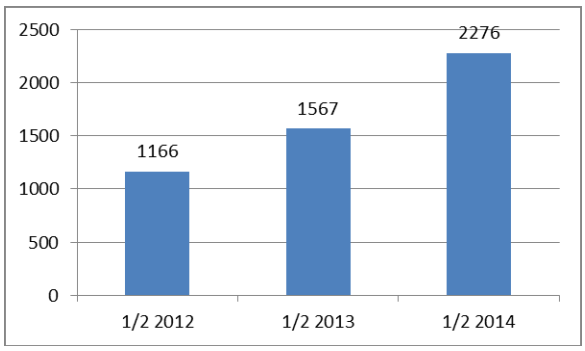
Policejní statistiky a jejich interpretace

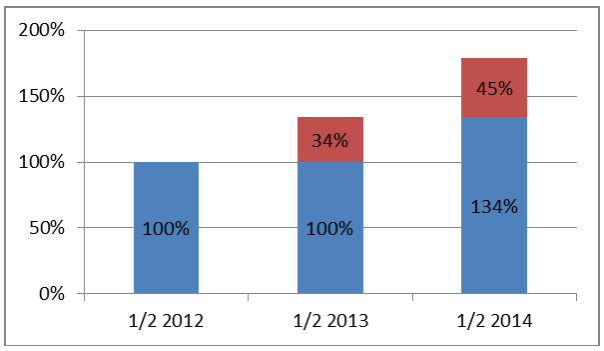
Kybernetická bezpečnost a kriminalita se v celoevropském měřítku dostávají stále více a více do centra pozornosti bezpečnostních složek i států jako takových. Vznikají národní týmy pro řešení kybernetických incidentů, specializované národní i mezinárodní policejní složky, připravuje se nová legislativa 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).

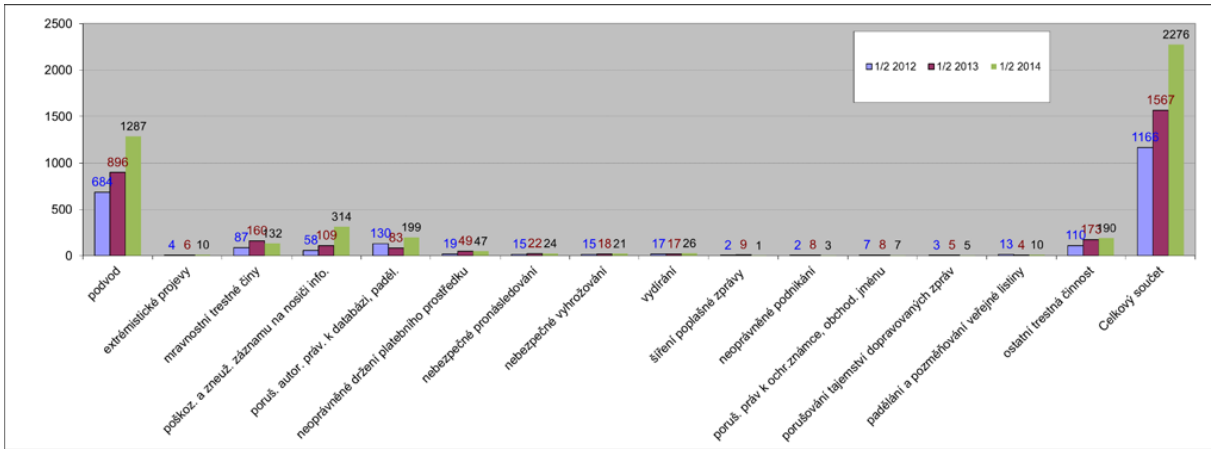
Také v prvním pololetí roku 2014 jsme byli svědky poměrně dramatického nárůstu počtu trestných činů, spáchaných s využitím informačních technologií. Počet zaregistrovaných skutků informační kriminality roste celosvětově už mnoho let a vzhledem k tomu, že stále větší část života a fungování společnosti se 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.



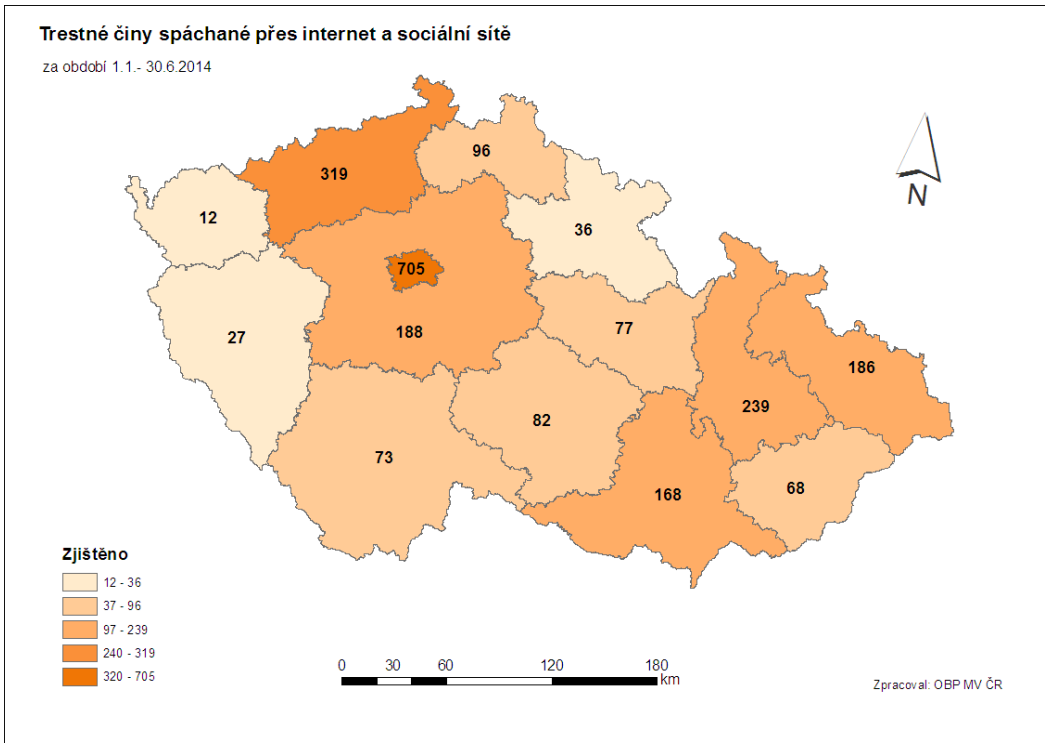


Z přiloženého grafu je dobře patrný meziroční nárůst incidence zaznamenaných případů informační kriminality, ve srovnání se stejným obdobím roku 2013. Porovnání s rokem 2012 vyznívá ještě nepříznivěji – česká policie musela v roce 2014 řešit o celé tři čtvrtiny více případů.

Naopak struktura zaznamenávané trestné činnosti se téměř nemění – stále výrazně dominují různé formy podvodného jednání, které i v první polovině roku 2014 tvořily necelou polovinu všech evidovaných skutků. S velkým odstupem pak následuje poškozování a zneužití záznamu na nosiči informací a různé mravnostní trestné činy (např. dětská pornografie). Ve sledovaném období řešila policie také 24 případů tzv. stalkingu (nebezpečné pronásledování), kde byla celá pětina případů zaznamenána v jinak málo exponovaném Libereckém kraji.



Co se týče geografického rozložení informační kriminality, pak také v roce 2014 přetrvává jednoznačná dominance Prahy, V metropoli je nahlášena celá třetina celkového nápadu této formy trestné činnosti. Oproti srovnatelnému období roku 2013 je překvapivý značný nárůst informační kriminality v Olomouckém kraji, který se po kraji Ústeckém dostal na nelichotivou třetí příčku (v roce 2013 byl přitom až na 7. místě a za celý rok zde došlo k menšímu počtu skutků, než za 1. pololetí 2014). V tuto chvíli přitom není zcela zřejmé, čím je tento regionální nárůst způsoben. Geografické rozložení nápadu informační kriminality znázorňuje následující mapa. V tomto ohledu je vhodné poznamenat, že vzhledem k prostorové neuchopitelnosti informační kriminality je geografické rozložení v rámci ČR spíše orientační.



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.

Masivně na vzestupu jsou útoky formou tzv. **phishingu**. Časté je zaznamenávání přístupových kódů, sloužících zejména k podvodnému přístupu na bankovní účty, z nichž jsou pak neoprávněně odčerpávány finanční prostředky), a to navíc za souběžného zneužití předem vytvořeného prostředí ve formě tzv. botnetů či proxy serverů jako např. TOR. Řadu těchto případů popisujeme v kapitole věnované bezpečnosti finančních institucí.

Na našem území původně nebyl častý výskyt organizátorů takovéhoto jednání a vyskytovali se spíše tzv. bílí koně „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. To, že jsou útoky často organizovány ze zahraničí, je často zřejmé ze špatné češtiny, kterou jsou psány hromadně rozesílané emailové zprávy, tvářící se jako oficiální informace od banky či pojišťovny. V poslední době jsou ale čím dál častěji zaznamenávány případy, kdy se části těchto organizovaných skupin přesouvají na naše území, případně je taková činnost řízena přímo z ČR.

Při najímání tzv. bílých koní pachatelé často zneužívají lidské důvěřivosti. Tito lidé jsou mnohdy vyhledáváni skrze klasické inzeráty s nabídkou práce, které se objevují i na seriózních portálech, nabízejících zaměstnání. Nabízejí obvykle časově zcela nenáročnou práci z domova na překvapivě vysoké pozici (např. manažer finančních operací) a přitom kladou na uchazeče jen minimální požadavky. Pro získání zaměstnání musí zájemce obvykle zaslat kopii občanského průkazu, na který pachatelé jeho jménem zakládají konta v bankách atd. V řadě finančních institucí lze totiž podobné úkony vyřídit korespondenčně, s pouhou kopií OP, což činnost pachatelů výrazně usnadňuje.

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 většina bílých koní vůbec netuší, že se podílí na ilegálních aktivitách, hrozí jim stíhání za podíl na legalizaci výnosů z trestné činnosti.

Lidská důvěřivost, hraničící v některých případech s naivitou, je vůbec obecně nejčastější vlastností, na které řada podvodníků zakládá své ilegální podnikání. Lidé jsou přitom v internetovém prostředí často mnohem méně opatrní, než v „reálném“ světě. Příkladem mohou být internetové inzeráty a aukce na prodej aut z ciziny – nabízejí kvalitní ojetiny za velmi výhodnou cenu s tím, že auto je např. v Anglii a požadují předem peníze na jeho transport do ČR. Po zaplacení se podvodníci dožadují dalších částek na různé nově vymyšlené výdaje. Podvedení lidé často odešlou peníze dvakrát i třikrát, než si uvědomí, že se stali obětí podvodu. Mnoho z nich přitom případ ani neohlásí na policii.

O něco náročnější je pro uživatele rozeznat falešné e-shopy, další z častých nešvarů českého internetu. Ty jsou obvykle zakládány na omezenou dobu a po pár týdnech beze stopy zmizí, aby se zase pod jinou grafikou a jiným názvem objevily jinde na internetu. 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.

Ve sledovaném období byly jednou z nejčastějších forem internetových podvodů v ČR hromadné emaily, upozorňující na narůstající dluh u některé ze zavedených bankovních institucí (jejich text je možné si přečíst v sekci „Vybrané události ve sledovaném období“). Jak takový útok probíhá, ukazuje případ ženy z Kroměřížska, která tímto způsobem přišla o 400 tisíc korun. Email, vyhrožující dlužnou částkou, obsahuje přílohu (označovanou jako faktura či smlouva), která skrývá virus, skrze nějž se pachateli podaří získat přihlašovací údaje do internetového bankovnictví. Krátce nato pachatel, opět jménem banky, kontaktuje oběť znovu, tentokrát však na mobilní telefon a žádá instalaci bezpečnostního programu. Jedná se opět o virus, který zprávu s autentizačním kódem přesměruje k útočníkovi. Tomu pak již nic nebrání převést přes internetové bankovnictví oběti libovolnou částku na vlastní účet.

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 často 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.

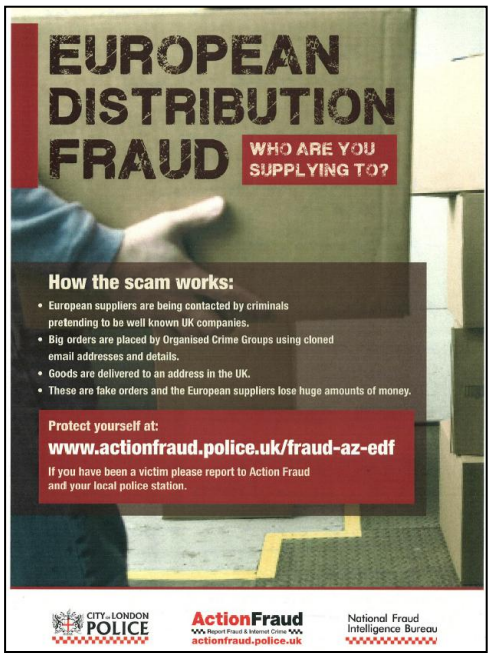
Pokud jde o oblast porušování autorských práv v prostředí informačních technologií, zůstává trend přesunu do segmentu datových úložišť. Výjimkou ve výměnných sítích je stále aktivní tzv. torrentová služba. Rovněž tak je zřejmé prolnutí nových technologií tzv. cloudových služeb, primárně určených ke sdílení elektronických dat mezi jednotlivými technickými zařízeními uživatele či určené pro potřeby vzájemného sdílení úzce komunitních a firemních skupin.

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 1. polovinu roku 2014 celkem 3522 podnětů směřovaných právě do oblasti kybernetického prostředí.

Abychom předešli dojmu, že česká policie je jediná, která se potýká s vysokým počtem podvodů v internetovém prostředí, můžeme uvést údaje z konference uspořádané britskou NFIB (National Fraud Intelligence Bureau) a City of London Police. V roce 2013 dosáhla v Británii celková škoda v souvislosti s trestnými činy, zahrnujícími firemní sektor, 43,5 mld. liber a britské policii bylo ohlášeno více než 402 tisíc případů podvodů.



Britská policie z tohoto důvodu spustila outsourcovaný projekt Action Fraud. Více než 100 operátorů přijímá v pracovních dnech hlášení ohledně různých druhů podvodů. Zároveň je poškozeným nepřetržitě k dispozici specializovaná webová stránka Action Fraud (actionfraud.police.uk). Měsíčně je prostřednictvím tohoto projektu ohlašováno 19 tisíc případů podvodů, z nichž velká část má souvislost s podvodnou inzercí na internetu či se zneužitím platebních karet.

Kvůli nejaktuálnější hrozbě, které v současnosti čelí mnoho evropských firem, byla dokonce spuštěna zvláštní osvětová kampaň. Organizované skupiny podvodníků kontaktují dodavatele v EU, a to zpravidla výrobce potravin, ale mohou oslovit i exportéry/výrobce z různých dalších odvětví. Vydávají se za představitele/zaměstnance velikých britských firem resp. obchodních řetězců. Komunikují prostřednictvím pozměněných či klonovaných emailových adres daných firem, kdy na první pohled může vypadat daná adresa důvěryhodně. Pro telefonickou komunikaci volí také telefonická čísla, která jsou velmi podobná oficiálně zveřejněným pravým telefonickým kontaktům uvedeným na oficiálních webových stránkách těchto známých společností.

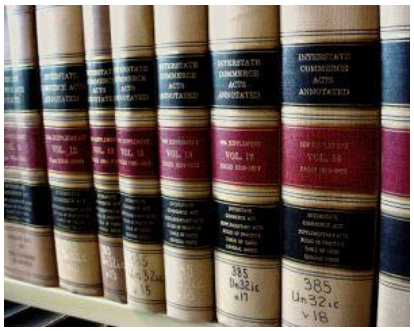
Organizované kriminální skupiny provedou objednávku a při dodání zpravidla udají adresu v UK, která buď nemá vůbec co do činění s domnělým velkým zákazníkem, nebo je místem doručení skutečná adresa skladů významné britské firmy. V takovém případě dostane na poslední chvíli (někdy i během samotné přepravy zboží) zahraniční exportér z britské strany pokyn ohledně změny doručovací adresy, kde si zboží následně převezmou podvodníci.

Tento typ podvodu není v zásadě zcela nový, skupiny organizovaného zločinu jej využívají již několik let. Nyní však britští kriminalisté zaznamenávají v souvislosti s vývojem informačních/telekomunikačních technologií další „vylepšení“ postupů podvodníků a především podstatné rozšíření těchto činů. V minulosti byl tento postup registrován v jednotkách či desítkách případů, nyní se jedná o řádově vyšší počet zaznamenaných trestných činů a škody dosahují značných finančních objemů.

Zákon o kybernetické bezpečnosti

Dlouho očekávaná právní norma, kterou se Česká republika zařadí mezi jedny z prvních států světa, které mají oblast kybernetické bezpečnosti upravenou speciálním zákonem, byla dne 2. ledna 2014 schválena vládou a 18. června s ní pak vyslovila souhlas Poslanecká sněmovna a následně také Senát. Nový zákon o kybernetické bezpečnosti tedy vstoupí v platnost v plánovaném termínu 1. ledna 2015. Tvůrcem zákona je Národní bezpečnostní úřad (NBÚ). Co je tedy jeho hlavním a účelem obsahem?

Cílem zákona je především ochrana důležitých informačních a komunikačních systémů státu (zejména pak těch, které jsou součástí kritické infrastruktury) z pohledu kybernetické bezpečnosti. Lze totiž očekávat, že právě z virtuálního prostoru budou tyto systémy v budoucnu nejvíce ohroženy.



Zákon se snaží držet několika hlavních zásad. Především vychází z předpokladu, že za bezpečnost vlastní sítě si odpovídá každý provozovatel sám. NBÚ pouze nastavuje obecné standardy, které by měl každý správce důležitého informačního či komunikačního systému plnit. Tyto standardy jsou technologicky neutrální, takže je na správci systému, jaké konkrétní řešení si pro jejich plnění zvolí. Zákon by tak neměl zvýhodňovat žádného konkrétního dodavatele. Zároveň se zákon snaží cílit zejména na státní správu a minimalizovat zásahy do práv soukromoprávních subjektů (ty pod zákon spadají pouze v případě, kdy jsou provozovateli kritické infrastruktury).

Jádrem zákona je standardizace bezpečnostních opatření nejdůležitějších informačních a komunikačních systémů státní správy tak, aby všechny splňovaly alespoň minimální bezpečnostní požadavky. Zároveň zavádí povinnost hlášení kybernetických incidentů nově vzniklému Národnímu centru kybernetické bezpečnosti v Brně, které bude tyto informace shromažďovat, vyhodnocovat a případně varovat další subjekty. Národní bezpečnostní úřad také může za určitých podmínek nařídit správci systémů vykonání určitých protiopatření (např. pokud se z jeho počítače s pomocí botnetu útočí na další systémy), konkrétní způsob jejich aplikace bude ale na správci samotném.

Zákon se nevztahuje na systémy, nakládající s utajovanými informacemi, které mají svou vlastní právní úpravu. Rozlišuje dvě hlavní kategorie systémů, které je potřeba chránit:

1. **kritická informační infrastruktura** – (KII) – je zejména taková, která je určitým způsobem navázána na stávající prvky kritické infrastruktury. Např. jaderná elektrárna potřebuje ke své činnosti nutně určité počítačové systémy, jejichž výpadek by pro ni znamenal ohrožení bezpečnosti. Případně sem lze zahrnout ty informační a komunikační systémy, které plní průřezová kritéria z nařízení vlády č. 432/2010 o kritické infrastruktuře (např. by jejich nefunkčnost způsobila ztrátu 0,5 % HDP, úmrtí většího množství osob atd.).

2. **významné informační systémy** – (VIS) - jsou systémy, které jsou velmi důležité pro chod státu a státní správy (jejich narušení by znamenalo pro stát problém při výkonu jeho základních činností), ale zároveň neplní kritéria pro zařazení do kritické informační infrastruktury (KII). VIS nebudou muset plnit tak přísné bezpečnostní standardy jako KII, ale i na ně se vztahuje např. povinnost hlásit bezpečnostní incidenty.

Správci KII a VIS (v drtivém případě se jedná o orgány státní správy, pouze některé prvky KII spravují soukromé subjekty, např. velké energetické firmy) budou muset zavést určitá organizační a technická opatření tak, aby jejich systémy byly řádně zabezpečené.

Zavedení a funkčnost těchto opatření bude kontrolovat NBÚ, který může případně ukládat i sankce (v prvním roce to bude jen formou upozornění, v dalších letech mohou ale následovat i pokuty).

Těchto opatření je celá řada - správce musí mít vytvořen organizační systém řízení bezpečnosti informací (kdo za co v bezpečnosti odpovídá, kdo jeho činnost kontroluje atd.), vypracovanou bezpečnostní politiku, analýzu rizik, standardy bezpečnosti pro externí dodavatele, bezpečnost lidských zdrojů, řízení a evidenci přístupu k citlivým datům, sledování síťového provozu, systém hlášení a řešení incidentů atd. Zároveň musí být systémy zabezpečeny i technicky (antivirový software, fyzická bezpečnost objektů a přenosových tras, šifrování atd.).

Zákon zároveň rozlišuje kybernetickou bezpečností událost a kybernetický bezpečnostní incident (právy ty se hlásí na NBÚ). Úřad může za určitých podmínek nařídit provozovateli vykonat protiopatření k odvrácení kybernetického incidentu či probíhajícího útoku. Správce systému jej pod hrozbou sankce musí splnit – bude ovšem obvykle ponecháno na jeho rozhodnutí, jakým způsobem tak učiní (zdali např. dočasně vypne celou svou síť, anebo zvolí méně drastickou metodu – důležitý je výsledek a tím je zastavení útoku). I po proběhnutém incidentu může NBÚ vydat dodatečné ochranné opatření, aby se podobná situace již neopakovala.

Za účelem přijímání hlášení, evidence incidentů a pomoci napadeným subjektům zákon uvádí dvě pracoviště – **vládní CERT**, který v Brně provozuje NBÚ a **národní CSIRT**, což je soukromý tým, který založila a provozuje společnost CZ.NIC. Národní CSIRT je starší, byl prvním obdobným týmem v ČR a vzhledem k jeho zkušenostem a etablovanému fungování byl na základě memoranda s NBÚ zahrnut do zákonem stanovené bezpečnostní architektury. CSIRT tuto funkci vykonává bezplatně. Na národní CSIRT se budou obracet jen soukromí provozovatelé KII, státní správa bude incidenty hlásit vládnímu CERTu.

Další novinkou v zákoně je tzv. **stav kybernetického nebezpečí**, který v mnoha aspektech připomíná klasické mimořádné stavy známé z krizového zákona (není ale jedním z nich). Vyhlašuje jej ředitel NBÚ v případě rozsáhlého ohrožení kybernetické infrastruktury státu a to nejdéle na 7 dnů (lze prodlužovat až na 30 dnů). Za tohoto stavu může NBÚ ukládat vykonání závazných protiopatření i těm soukromým subjektům, na které se jinak zákon nevztahuje (ale jen těm, o kterých mluví zákon o elektronických komunikacích – jsou to např. telekomunikační firmy atd.).

Bezpečnostní standardy, které musí jednotlivé subjekty plnit, nestanovuje zákon, ale tzv. **standardizační vyhláška**, kterou NBÚ v nedávné době dokončil a nyní bude projednána v meziresortním připomínkovém řízení.

Nové hrozby v oblasti kybernetické bezpečnosti

Nová hrozba: zavirované routery

V průběhu května 2014 se začaly po celé České republice objevovat případy **napadení routerů** poměrně sofistikovaným virem. Podle bezpečnostních expertů i policejních detektivů se jedná o **jednu z nejzákeřnějších hrozeb na českém internetu poslední doby**. Na rozdíl od většiny běžných útoků, které v drtivé většině případů využívají lidské důvěřivosti či nepozornosti, proti této formě útoku jsou běžní uživatelé prakticky bezbranní, a to dokonce i tací, kteří jinak dodržují zásady bezpečného pohybu na internetu.

Routery (směrovače) jsou v podstatě základní kameny domácích i firemních sítí. Právě skrze ně se počítače v síti zapojené připojují k internetu a komunikují mezi sebou. Útoky na routery nejsou úplnou novinkou, tento je ale jeden z prvních, který dokáže překonat i silné heslo, nastavené uživatelem (přesto se doporučuje si kvalitní heslo na routeru nastavit, protože to odrazí většinu běžných útoků).

V minulé situační zprávě jsme informovali o rizicích spojených s užíváním mobilních zařízení. Obecně jsme konstatovali, že zabezpečení mobilních zařízení stále pokulhává za bezpečností klasických stolních PC. V souvislosti s květnovými odhaleními ale někteří analytici začínají hovořit o tom, že ještě více než mobilní zařízení **jsou do budoucna velkou bezpečnostní slabinou zařízení síťová** (jako právě routery), které jsou navíc pod minimální kontrolou uživatelů (většinou jde o „krabičku“, kterou uživatel jednou zapojí a po celé roky o ní ani neví). Na síťových zařízeních navíc v drtivé většině případů neprobíhají žádné automatické aktualizace, takže pokud se na nich objeví nějaká zranitelnost, zůstane otevřená po celou dobu jejich provozu. Manuálně si totiž záplaty na routerech téměř nikdo neinstaluje a antivirus, nainstalovaný v PC, často router nekontroluje. Až současná vlna útoků by mohla vést výrobce k lepšímu zabezpečení a případnému zavedení automatických aktualizací.

Jak takový útok na směrovače vlastně probíhá? Router se může nakazit virem od jiného, již infikovaného zařízení, případně při procházení napadených internetových stránek. Virus v routeru v podstatě ovládne internetové připojení pro všechna zařízení v síti (nemusí se přitom jednat jen o PC, ale i o mobily a tablety připojené přes wi-fi) a může bez jeho vědomí přesměrovat uživatele na libovolné internetové stránky.

V minulých situačních zprávách jsme varovali před falešnými stránkami internetového bankovnictví, které zneužívají překlepů při zadávání adresy (např. místo „servis24.cz“ uživatel chybně zadá „sevris24.cz“). V případě napadení routeru ale uživatel nemá sebemenší možnost ovlivnit, kam se připojuje, takže i pokud zadá adresu známého portálu správně (např. google.cz, seznam.cz), je přesměrován na falešné stránky se stejnou grafikou. Možností zneužití tohoto principu se nabízí celá řada - v případě nedávných útoků to byla pokračující snaha dostat virus z routeru do počítače (či mobilu) uživatele. Na stránkách, kterým uživatel důvěřoval, ale které byly ve skutečnosti falešné, se objevila výzva k aktualizaci flash playeru. Tato aktualizace obsahovala malware.

Je potřeba zdůraznit, že samotné stránky (např. právě Seznamu či Googlu) vůbec napadeny nebyly. Infikovaný router pouze zfalšoval jejich URL adresy, takže uživatel netušil, že

namísto těchto známých portálů přistupuje na úplně jiné stránky. Původní stránky (např. seznam.cz) přitom infikovaný router zcela zablokoval, takže bez odstranění viru nebylo možné se k nim připojit. Odhalit virus v routeru přitom pro běžného uživatele není snadné. Jednou z možností je porovnat vzhled a chování stránek na PC a na mobilním telefonu (připojeném přes mobilní síť, nikoliv wi-fi!). Pokud po Vás internetové stránky na PC vyžadují nestandardní aktualizace, případně se Vám jeví podezřelá jejich podoba či obsah a na mobilním telefonu je obsah stejných stránek v pořádku, je s největší pravděpodobností chyba právě ve Vašem směrovači.

Nejsnazším způsobem odstranění viru z routeru je uvedení tohoto zařízení zpět do továrního nastavení (obvykle se provádí stiskem malého tlačítka „reset“ s pomocí tužky či kružítka). Následně je nutné nastavit si pro router silné heslo (pro bezdrátová zařízení i silné heslo pro wi-fi připojení). Bohužel, návrat do továrního nastavení sice router viru zbaví, nezaručí ale, že zařízení nebude opět stejným způsobem napadeno v budoucnu. Je proto vhodné následně zkontrolovat u výrobce zařízení, zdali na danou hrozbu již nevydal bezpečnostní záplatu a tu pak dle jeho instrukcí manuálně nainstalovat. Krajním řešením může být i nákup jiného typu routeru.

Útoky na routery nejsou zdaleka jen problémem České republiky. Od počátku roku 2014 se objevuje množství případů také v Polsku, Německu, Velké Británii či v USA. Objevení této nové zranitelnosti, proti které se jen pomalu vyvíjí účinná obrana, si přes internetová fóra sdílejí hackeři po celém světě, a je tak pravděpodobné, že tyto útoky budou stále častější do doby, než se podaří doposud opomíjenou bezpečnost síťových zařízení zlepšit.

Chyba krvácejícího srdce

Celosvětově bylo zřejmě nejvýznamnější a nejdiskutovanější bezpečnostní událostí první poloviny roku 2014 odhalení **závažné chyby v šifrovací knihovně OpenSSL**, která brzy získala přezdívku **Heartbleed Bug** („chyba krvácejícího srdce“).

Knihovna OpenSSL se používá k ochraně dat při jejich internetovém přenosu a kvůli jejímu rozšíření je považována za jeden ze základních kamenů internetu. Používají ji webové servery, elektronická pošta, internetové bankovnictví, chatovací programy atd. Podle některých odhadů se tak mohla chyba dotknout až **dvou třetin všech internetových stránek**.

Problém odhalili na počátku dubna analytici firmy Google ve spolupráci s bezpečnostní společností Codenomicon. Jelikož si uvědomili, jak velké dopady by mohlo mít její zveřejnění na bezpečnost internetu, zpráva o chybě byla vydána s několikadenním zpožděním, aby měli správci knihovny více času na její opravu. Případní útočníci totiž mohli díky této zranitelnosti získat přístup k nešifrovaným datům, heslům a přístupovým kódům, ale také např. k zabezpečené emailové komunikaci.

Dlouho přitom nebylo jasné, zda se jednalo o potenciální hrozbu, anebo této zranitelnosti skutečně někdo zneužil. V tomto případě by totiž případný útok nezanechal žádné zjevné stopy. Prakticky všechny významné servery začaly samozřejmě okamžitě využívat novou, opravenou verzi knihovny, přesto byli uživatelé knihovny vyzváni k preventivní změně hesel a přístupových údajů, ve všech službách využívajících OpenSSL.

Zdali ale chybu před analytiky Googlu a vydáním bezpečnostní záplaty odhalili i nějací hackeři, není stále zřejmé. V polovině dubna se v Kanadě objevil případ 19letého hackera, který Heartbleed Bug prokazatelně využil k **prolomení systému kanadského finančního úřadu**. Podařilo se mu ukrást čísla zhruba 900 pojištěnců. Mladíka zadržela policie, při vyšetřování nicméně vyšlo najevo, že se o chybě dozvěděl až po jejím zveřejnění a využil toho, že finanční úřad dostatečně rychle svou knihovnu neaktualizoval.

Agentura Bloomberg zase v dubnu přinesla zprávy, že o chybě věděla a dlouhodobě ji ke špionáži využívala americká Národní bezpečnostní agentura (NSA), veřejnosti známá především kvůli aféře kolem Edwarda Snowdena. Bloomberg se opíral o nespecifikované „zdroje z prostředí zpravodajské komunity". Okamžitě se objevily spekulace, že šlo o cíleně vytvořenou zranitelnost, která fungovala jako tzv. backdoor (zadní vrátka) pro zpravodajské služby. Nic z toho ovšem nebylo oficiálně potvrzeno. NSA popírá, že by tuto zranitelnost jakkoliv v minulosti využívala.

Ve skutečnosti tedy neexistují žádné důkazy o tom, že by v souvislosti s chybou krvácejícího srdce došlo před jejím odhalením k nějaké ztrátě dat. Také Česká bankovní asociace oznámila, že nemá žádné zprávy o možném zneužití internetového bankovnictví touto cestou. Preventivní změna hesla ale může tuto skutečnost jedině pojistit. Britská BBC označila Heartbleed bug za **jednu z nejzávažnějších bezpečnostních trhlin v historii internetu**. Rozsah potencionálních škod (které ale podle všeho nakonec naštěstí nenastaly), šokoval i mnohé odborníky. Pozitivní zprávou ovšem je, že knihovna Open SSL je nyní pod mnohem lepším dohledem než dosud, neboť vzniklo hned několik nezávislých iniciativ, které ji testují proti objevení možných dalších zranitelností.

Další odhalené hrozby

První polovina roku 2014 byla všeobecně bohatá na odhalení závažných bezpečnostních mezer v rozšířených a často používaných zařízeních a programech. Krátce po zveřejnění chyby krvácejícího srdce přiznala firma Microsoft **závažný „zero-day-exploit" u všech verzí prohlížeče Internet Explorer**. Bezpečnostní záplata byla vydána s několikadenním odstupem, skrze chybu bylo přitom možné ovládnout celý počítač oběti.

Zranitelnost opět využívala Adobe Flash plugin a byla opravena v rámci mimořádné aktualizace (což jen dokládá důležitost pravidelných aktualizací nainstalovaného softwaru). Zranitelnost spočívá v tom, že Internet Explorer přistupuje do paměti i k objektům, které byly již smazány nebo chybně přiděleny. Útočník může podstrčit nakaženou stránku, která této chyby využije a dokáže tak spustit v Exploreru libovolný programový kód se stejnými právy, jako má jeho uživatel. Internet Explorer je přitom celosvětově jedním z nejrozšířenějších prohlížečů.

Ve sledovaném období zároveň přestala firma Microsoft podporovat svůj historicky vůbec nejúspěšnější operační systém – **Windows XP**. Nadále již pro něj nebude vydávat žádné bezpečnostní záplaty ani aktualizace, což jej do budoucna činí mimořádně zranitelným. Zdaleka ne všichni uživatelé tohoto oblíbeného operačního systému přitom spěchají s jeho výměnou, podle některých průzkumů si jej až 20 % klientů oblíbilo natolik, že se jej chystají používat i po zastavení podpory. Něco takového ale firma ani bezpečnostní experti silně nedoporučují – jakákoliv odhalená zranitelnost totiž už nadále nebude opravována a skalní fanoušci XP, kteří odmítli přejít na novější systémy, tak budou již natrvalo vystaveni na milost a nemilost hackerům.

Doslova záplava kyberútoků se v roce 2014 odehrála také v souvislosti s **krizí na Ukrajině**. Konflikt se postupně přeléval také do kybernetického prostředí a měl nejčastěji podobu DDoS útoků proti konkurenčním zpravodajským serverům. Napadené webové stránky jsou pak po nějaký čas nedostupné a znepřátelené hackerské komunity tím bojují proti „propagandě“ soupeře.

Náročnější útoky internetové stránky neznepřístupňují, ale rovnou modifikují jejich obsah. Neznámým hackerům se tak například podařilo prolomit stránky Kremlem financované agentury Russia Today a změnit v článcích o ukrajinském konfliktu všechny varianty slova „Rusové“ na termín „nacisti“.

Ruské hackerské komunity byly přitom svým „vlasteneckým“ aktivismem známy již v minulosti. Velkému množství útoků čelily v minulosti (v době časů konfliktů a napjatých vztahů s Ruskem) také Estonsko a Gruzie. Ukrajinští hackeři ale v tomto případě nezůstávají svým ruským kolegům mnoho dlužní a na internetu tak zuří podobně intenzivní konflikt, jako na válečném poli ve východní Ukrajině.

Na závěr je možné se zmínit o dalším z trendů blízké budoucnosti, kterým je využití chytrých mobilních přístrojů, o kterém informuje portál týden.cz. Velký nástup využívání mobilních zařízení pro DDoS útoky lze očekávat vybudováním a spuštěním LTE sítí, které nabídnou dostatečnou rychlost mobilního připojení srovnatelnou se stávajícím pevným připojením.

Fotbal – příležitost pro hackery

Velké mezinárodní události, jako jsou olympijské hry či fotbalové mistrovství světa, přirozeně přitahují pozornost celé řady podvodníků a hackerů. Společnost Trend Micro odhalila celé čtyři stovky různých aplikací, které se tvářily, že mají souvislost s fotbalovým šampionátem, ale ve skutečnosti obsahovaly nebezpečný malware. Podobně se objevil nespočet falešných internetových stránek, podvodných internetových prodejců lístků atd. Fotbaloví fanoušci by se proto před příštím mistrovstvím měli mít na pozoru, což se ostatně týká i všech dalších velkých sportovních událostí.

Zjistit, že se počítač, tablet nebo mobil stal součástí botnetu, který je pak zdrojem útoků, je velmi obtížné. Majitel telefonu to zpravidla může poznat podle objemu dat, které jsou bezdůvodně a nestandardně odesílané, na výši svého účtu nebo podle velmi rychle vybité baterie. Škodlivý kód je obvykle aktivován na dálku a chytrý telefon se na pokyn hackera stává součástí botnet sítě jen po určitou dobu.

Riziko kybernetických DDoS útoků se zvyšuje každým dnem, nicméně po zprovoznění LTE sítí v širokém měřítku, bude snadnější mobilní zařízení zneužít. Dnešní mobilní telefony disponují výkonem srovnatelným s osobními počítači před několika lety. Palčivý problém to bude zejména pro mobilní operátory, kteří by měli již nyní investovat do technologií, které jim umožní DDoS útoky z chytrých telefonů účinně eliminovat. Zároveň se budou muset zaměřit na detekci neznámých škodlivých kódů, které se budou v mobilních sítích šířit.

Vybrané události ve sledovaném období

Leden

Americká NSA sledovala po světě speciálním softwarem přes 100 tisíc počítačů

Americká Národní agentura pro bezpečnost (NSA) sledovala téměř 100.000 počítačů v cizích zemích pomocí speciálně vytvořeného programu. Tajná technologie založená na použití rádiových vln umožnila NSA získat přístup k jinak dobře chráněným počítačům například v EU, Rusku či Číně, napsal deník The New York Times. Kvůli aféře se sledováním komunikace doma i ve světě nyní řeší prezident Obama možné změny v budoucích praktikách vládní tajné služby.

NSA podle deníku několik let používala speciálně vytvořený software, který pracoval s rádiovými vlnami a do počítačů se dostával například z USB karet tajně instalovaných do těchto strojů. Dlouhodobě tímto způsobem prý monitorovala počítače čínské či ruské armády, drogových kartelů, ale i některých úřadů uvnitř Evropské unie nebo svých asijských spojenců v boji proti terorismu. Deník ve své zprávě čerpá z interních dokumentů NSA či informací od amerických činitelů a počítačových expertů. Agentura nazvala tento program 'aktivní obranou' a mezi jeho nejčastější cíle patřilo čínské vojsko, které Washington obviňoval z opakovaných kybernetických špionáží.

Obří krádež přístupových účtů k emailům v Německu

Spolkový úřad pro bezpečnost v informačních technologiích (BSI) oznámil, že se neznámým pachatelům podařilo ukrást přístupová data k 16 milionům e-mailových účtů. Drtivou většinu z nich přitom vlastní němečtí uživatelé internetu.

Krádež byla zjištěna při analýze botnetových sítí, kterou úřad prováděl. BSI vzápětí zřídil i webové stránky, kde si uživatelé mohli ověřit, zda byl napaden i jejich účet. Krátce po svém zveřejnění ovšem stránky pro velký nápor zájemců zkolabovaly. Úřad také doporučil všem napadeným uživatelům, aby pokud možno nepoužívali vždy stejné heslo pro přihlašování do různých platforem (e-mail, sociální sítě, internetové bankovnictví atd.).

První Čech uvězněn za softwarové pirátství

Muž z Mostecka se stal historicky prvním Čechem, který dostal nepodmíněný trest vězení (20 měsíců) za šíření nelegálních kopií softwaru společností Microsoft a Adobe. Software opakovaně inzeroval v internetových bazarech za velmi nízké ceny a peníze inkasoval bezhotovostním převodem či na dobírku. Přišel si tak nejméně na 89 tisíc Kč, škoda výrobcům ovšem přesahuje půl milionu korun. Tu musí dle rozhodnutí soudu v plné výši uhradit.

Podle mezinárodní organizace Business Software Alliance (BSA), která se soustředí mj. na boj proti nelegálnímu užívání počítačových programů, se v ČR pirátsky užívá až 35 % softwaru v celkové hodnotě kolem 3,8 miliardy korun. Valná většina programů nabízených na internetových fórech a aukčních portálech jsou přitom právě nelegální kopie v různé kvalitě provedení. Je přitom důležité si uvědomit, že autorské právo v tomto případě neporušují jen ti, kteří takové software nabízí, ale i ti, kteří si jej koupí a nainstalují.

Únor

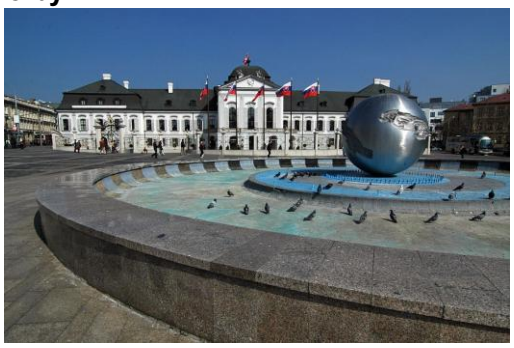
Španělé představili telefon, který má ochránit před špionáží

Španělský Geeksphone ve spolupráci se společnostmi Silent Circle a Pretty Good Privacy představil na veletrhu v Barceloně nový telefon, který cílí na uživatele s velkou starostí o své soukromí. Jeho součástí je nadstavba standardní verze systému Android, která umožňuje šifrování hovorů i SMS, ochranu dat a navíc monitoruje chování jednotlivých aplikací a jejich přístupová práva. Šifrované je také připojení k internetu. Telefon by tak teoreticky měl nejen zabránit odposlechům, ale bránit např. také personalizované reklamě.

Cena telefonu nicméně vzhledem k jeho ostatním parametrům (patří do střední třídy obdobných zařízení) zůstává dosti vysoká a produkt je tedy zaměřen na velice specifickou cílovou skupinu, pro které je ochrana jejich soukromí primárním parametrem při koupi. Některé bezpečnostní složky vyjadřují obavy ze zneužití obdobných zařízení organizovanými zločineckými skupinami a teroristy, sdružení prosazující maximální svobodu internetu naopak rozšíření těchto produktů vítají.

Březen

Hackeři se pokusili ovlivnit slovenské prezidentské volby



Slovenský prezidentský kandidát Robert Fico krátce před volbami na internetu oznámil, že vzdává boj o prezidentské křeslo. Na jeho oficiálních stránkách se objevil text s následujícím zněním: „S pokorou se vzdávám kandidatury na funkci prezidenta Slovenské republiky. Domnívám se, že právě v tomto okamžiku mého života nadešel čas na sebereflexi a na splnění mého slibu, že v roce 2014 už v politice nebudu. Cítím, že bych měl složit účet ze všeho špatného, co jsme způsobili. Upřímně mě to všechno mrzí. Děkuji za vaši důvěru a věřím, že společně nalezneme cestu, jak to napravit.“ Za tímto oznámením ale ve skutečnosti stál útok hackerů, kterým se podařilo stránky slovenského premiéra nabourat. Kvůli útoku podal Fico k Ústřední volební komisi podnět pro porušení volebního i trestního zákona. Podle něj byla hackerskou akcí významným způsobem narušena rovnost prezidentských kandidátů. Strana Smer-sociální demokracie označila útok neznámého hackera za vrchol agresivní antikampaně namířené proti Ficovi.

První kolo přímé prezidentské volby, které následovalo krátce po útoku, Fico nicméně vyhrál. Po porážce ve druhém kole se ale slovenským prezidentem nestal a hlavou státu se stal jeho soupeř Andrej Kiska.

Duben

Zavirované emaily varují před vysokými dluhy u bank

V dubnu se začaly českým internetem šířit ve velkém nevyžádané zprávy, které pod hlavičkou velkých bankovních institucí varují před dlužnými částkami v řádu několika tisíců korun. Příloha (údajná faktura či smlouva, ovšem se spustitelnou koncovkou „.exe“) však obsahuje virus. S touto formou malware si sice některé antivirové programy dokáží poradit, na stránkách národního bezpečnostního týmu CSIRT bylo nicméně možné nalézt návod na případné odstranění viru. Podvodný email byl nicméně poměrně dobře rozpoznatelný, neboť byl psán špatnou češtinou a obsahoval některé nesmyslné údaje.

Ukázka textu podvodného emailu:

Vážený zákazníku,
Jsme velmi rádi, že jste vyuziváli produktu z naší banky. Dovolujéme Vás upozornit, že k 25.04.2014 dlužné částky na osobní účet ve vysi #9471254734256890 9292.12 Kč. Nabízíme vám dobrovolně uhradit pohledávku v plné výši do 13.05.2014.
Dobrovolné uhrazeni pohledávky a dodrženi smlouvy #22365A830317939E umožňuje Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.
V případě prodlení uhrady pohledávky 9292.12 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základe pohledávky.
Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_22365A830317939E.zip"
S pozdravem,
Vedoucí odboru vymahani pohledávek
Adam Bejšovec

V červnu se objevila další, mnohem nebezpečnější verze tohoto útoku. Podoba infikovaného emailu zůstává prakticky stejná, je ale psán o něco lepší češtinou a obsahuje pokročilejší virus, který v dané době ještě antivirové programy nedokázaly odhalit.

Země NATO nacvičovaly kybernetickou válku

Severoatlantická aliance zorganizovala netradiční cvičení zabývající se hrozbou kybernetické války, kterého se zúčastnilo na 300 jednotlivců a týmů ze 17 členských zemí. Podle agentury Reuters šlo o simulaci útoku jedné fiktivní země na druhou, který vedlo 50 zkušených počítačových odborníků. Hrozbou pro internetové systémy již podle expertů nejsou osamělí hackeři či skupiny takových jedinců, ale jednotlivé státy, které do tohoto odvětví investují nemalé prostředky.
Akce se konala formálně v zemi, která se v roce 2007 v podobném konfliktu ocitla: Estonsko, které je členem NATO od roku 2004 a které patří k počítačově nejvyspělejším zemím světa, bylo terčem mohutných počítačových útoků, jež na několik dní ochromily servery místních úřadů a společností. Kybernetický nápor vypukl poté, co byl z centra Tallinnu přemístěn rozporuplný památník na oslavu Rudé armády, který byl postaven po druhé světové válce. Tallinn tvrdil, že počítačové útoky v roce 2007 pocházely z oficiálních ruských serverů, což Moskva popřela. Nynější cvičení, kterého se týmy účastnily ze svých domovských zemí včetně Česka, simulovalo podobné okolnosti včetně blokování některých webových stránek a vykrádání dat z e-mailových adres.

Počet případů kybernetické špionáže ve světě každým rokem roste

Počet případů počítačové špionáže ve světě se za poslední rok výrazně zvýšil. Podle dnes zveřejněné výroční zprávy americké komunikační společnosti Verizon za to může zvýšená aktivita v této oblasti ze strany různých skupin a vlád ve východní Evropě. Oběťmi elektronické špionáže jsou z více než poloviny cíle ve Spojených státech, uvedla agentura AP. Od loňské zprávy odborníci zaznamenali 511 hackerských útoků zaměřených na špionáž, což je třikrát více než v předchozích 12 měsících. Nejvíce, 49 procent, jich přišlo z Číny a dalších jihoasijských zemí. Na druhém místě s 21 procenty jsou východoevropské státy, především rusky mluvící země. Pět procent útoků přišlo z jiných míst a u 25 procent případů počítačové špionáže nelze určit zemi původu. Za 87 procenty případů elektronické špionáže stojí vlády, v ostatních případech různé skupiny, především zločinecké, které se snaží získané informace prodat, uvedli ve zprávě vyšetřovatelé z firem Verizon, Intel, McAfee, Kaspersky Labs a dalších soukromých společností a státních agentur.

Květen

Nová forma útoků cílí na routery a je běžným uživatelem prakticky neodhalitelná

Za určitý zlom v moderních formách kybernetických útoků označují někteří experti nový malware, který se začal nejpozději v průběhu května šířit také v ČR. Routery jsou základní stavební kameny domácích i firemních sítí a jejich prostřednictvím se útočníci snadno dostanou do všech připojených PC. Protože se virus často nenachází přímo v koncovém počítači, běžný uživatel ji prakticky nemá šanci odhalit. O tomto nebezpečném novém trendu blíže informujeme v analýze v úvodu této kapitoly.

Velký útok na největší aukční server eBay

Neznámým hackerům se podařilo provést úspěšný útok na největší aukční server světa, portál eBay. Odcizili při něm zhruba 145 milionů přístupových hesel. Firma vzápětí vyzvala všechny své uživatele ke změně přístupových údajů, zároveň ale čelí kritice, že o útoku, který se odehrál již na přelomu února a března, informovala až v květnu.

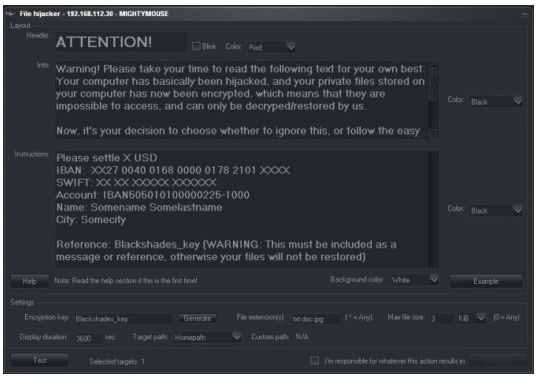
Platební brána PayPal, kterou eBay také vlastní, při útoku podle všeho ohrožena nebyla. Hackeři se ale dostali k přístupovým heslům, emailovým i fyzickým adresám a datům narození řady uživatelů. Do vnitřní sítě eBay se útočníkům podařilo proniknout díky odcizeným zaměstnaneckým účtům, které zřejmě získali od neopatrných pracovníků aukčního portálu.

Celosvětová operace proti hackerům kolem malwaru BlackShades

Během dvoudenní operace, která probíhala v 16 zemích celého světa (kromě 10 států EU také v USA, Kanadě, Chile, Chorvatsku, Moldavsku a Švýcarsku) se bezpečnostním složkám podařilo rozbít kriminální síť tvůrců, prodejců a uživatelů nebezpečného malwaru BlackShades. Skupina hackerů vyvinula tento virus, který byl schopen zcela ovládnout počítač oběti (zajistit přístup k dokumentům a fotografiím, zaznamenat zadávaná hesla, dokonce používat webkameru bez vědomí uživatele) a následně jej na černém trhu prodávala dalším zájemcům. Upravená verze viru sloužila i jako ransomware a obdoba známého Cryptolockeru (zašifrovala data na počítači a požadovala výkupné).

Koordinační skupině, ve které byli mj. zástupci Europolu, Eurojustu, FBI a nového Evropského centra kybernetické kriminality (EC3), se podařilo dovést do úspěšného konce dvoudenní akci mnoha národních policejních složek, při které bylo provedeno 359 domovních prohlídek a bylo zatčeno přes 80 osob. Zabaveno a zanalyzováno bylo přes 1100 různých elektronických zařízení (počítače, mobilní telefony, datová úložiště atd.), krom toho byly při domovních prohlídkách odhaleny také nelegálně držené zbraně a drogy. V České republice tato mezinárodní policejní akce neprobíhala.

Akce necílila jen na tvůrce malwaru, ale i na jejich zákazníky, kterým byl virus za úplatu přeprodáván. Ti jej totiž vesměs využili k ilegálním aktivitám. Příkladem může být 18letý mladík z Nizozemska, kterému se podařilo s BlackShades proniknout do zhruba 2000 počítačů. Bez vědomí jejich majitelů pořizoval snímky žen a dívek z dálkově ovládnuté webkamery, které pak dále distribuoval.



Červen

Společnost Google začala ze svých vyhledávačů vymazávat první občany EU

Společnost Google začala v červnu plnit rozhodnutí Soudního dvora EU, který potvrdil právo uživatelů internetu být na této celosvětové síti „zapomenut“. Rozhodnutí padlo na základě stížnosti jednoho španělského občana, kterému vadilo, že Google ve výsledcích vyhledávání zobrazuje článek z deníku z roku 1998, v němž se píše o dražbě jeho nemovitosti z důvodu dluhů na sociálním zabezpečení. Španěl argumentoval tím, že dluh již dávno uhradil a tato nadále irelevantní informace jej může v současnosti poškodit.

Španělský úřad pro ochranu údajů zamítl stížnost proti vydavateli deníku, který informaci zveřejnil legálně. Vyhověl však ve stejné věci ve vztahu ke společnosti Google a její španělské pobočce. Ty se ale odvolaly k soudu, který se Evropského soudního dvora dotázal na jeho výklad evropské směrnice o ochraně osobních údajů. Ten konstatoval, že jde o zásah do základních práv evropských, a že vyhledávače nesmí irelevantní informace nadále indexovat.

Jedná se o významný precedens, který může mít poměrně rozsáhlé dopady. Rozhodnutí se pochopitelně netýká pouze Googlu, ale všech vyhledávačů, nabízejících své služby na území Evropské unie (bez ohledu na to, ve které zemí sídlí). Kritici označují rozhodnutí soudu za cenzuru a snahu o vymazávání historie, jejímž důsledkem bude, že o vymazání nepohodlných údajů budou žádat politici a zločinci. Zastánci verdiktu jej hájí tím, že soud vyňal ze svého rozhodnutí odkazy, u nichž právo veřejnosti na informace převažuje nad právem jednotlivce na soukromí. Google v květnu v rámci implementace soudního rozhodnutí zveřejnil online formulář, kde budou lidé moci o vymazání příslušného výsledku vyhledávání zažádat. Oprávněnost žádosti a neaktuálnost zobrazované informace přitom posoudí sama firma, v případě nesouhlasu s jejím rozhodnutím je možné se obrátit na dozorčí a soudní orgány. Během prvních čtyř dnů obdržel Google v tomto směru přes 40 tisíc podnětů.

Poskytovatelé internetu žalují britskou zpravodajskou službu

Několik firem podnikajících v oblasti internetu podalo společnou žalobu proti britské službě GCHQ (Government Communications Headquarters), která podle nich podnikala cílené hackerské útoky proti jejich infrastruktuře za účelem kybernetické špionáže. Podle těchto společností tak byla narušena důvěra jejich zákazníků v soukromí jejich dat, přičemž právě na této důvěře firmy zakládají své podnikání. Obvinění navazuje na odhalení Edwarda Snowdena, který na praktiky britské GCHQ upozornil. Podle jeho zpráv zahrnovaly také spear phishing proti zaměstnancům a infekci špionážním malware. GCHQ úzce spolupracovala s americkou NSA. Cílem útoků měly být i telekomunikační firmy (např. belgický Belgacom). Jedná se o vůbec první žalobu tohoto typu proti britské zpravodajské službě.

Některé nástroje, vyvinuté či používané GCHQ, popsal list The Guardian. GCHQ údajně využívá program Gateway, který umožňuje uměle zvýšit návštěvnost stránky či sledovanost videí na YouTube. Dále programy Underpass, s nímž lze měnit výsledky webových hlasování, Spring Bishop, který vyhledává „soukromé fotografie cílů na webu“. Jiné nástroje odstraňují veřejné informace z Twitteru, Facebooku, Googlu+, Linkedinu a YouTube, nebo je tam naopak automaticky umisťují. Stejně nebo podobně fungující programy přitom používá i řada hackerů.

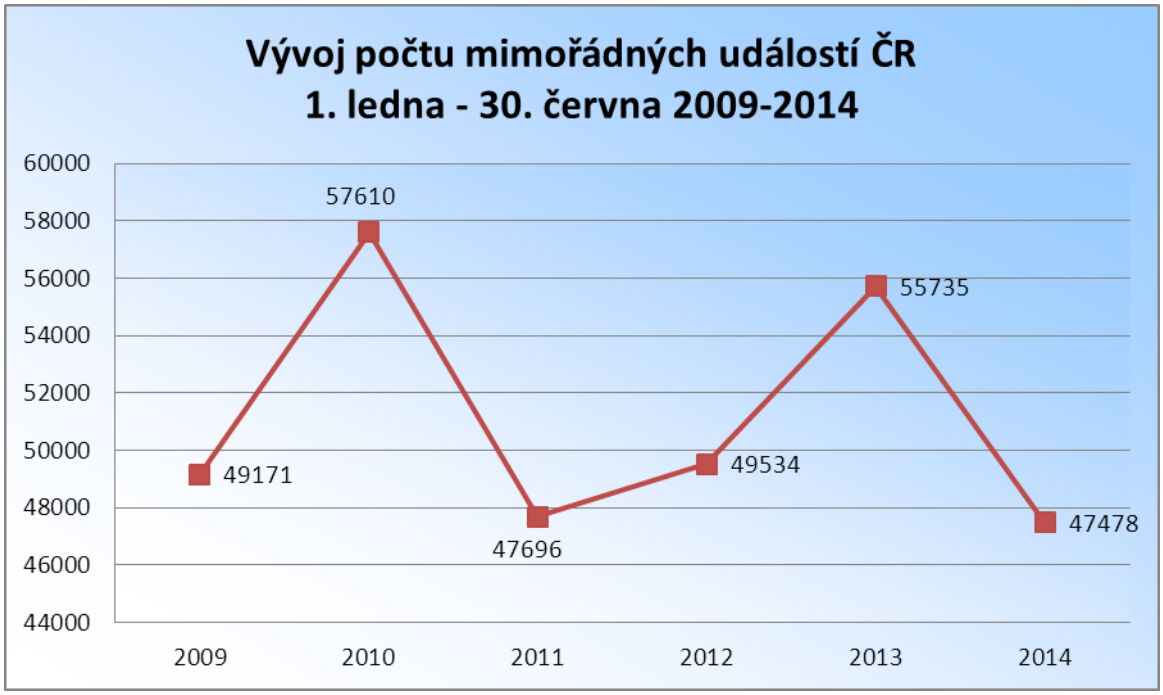
Zdroje pro tuto kapitolu: cleverandsmart.cz, PČR, ČTK, MZV, sxc.hu, idnes.cz, europol.europa.eu,aphaia.co.uk, allpremium4.blogspot.com, aktualne.centrum.cz, govcert.cz, lidovky.cz, novinky.cz, technet.idnes.cz, zive.cz, e15.cz, trustport.com, csas.cz, kickstarter.com, interpol.int, hpsolutions.cz, economist.com, 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.

KRIZOVÉ ŘÍZENÍ

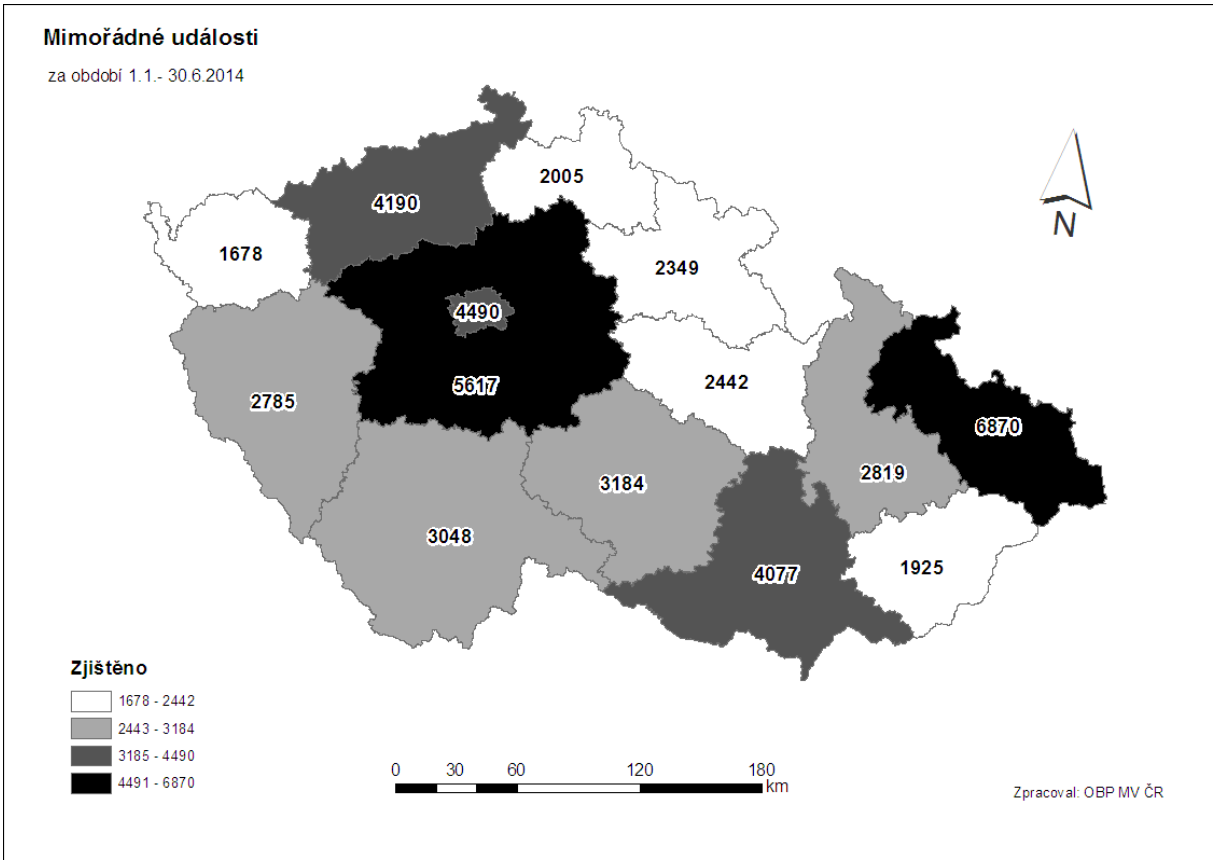
Hasičské statistiky a jejich interpretace

Namísto policejních statistik se v tomto případě soustředíme na statistiky Generálního ředitelství Hasičského záchranného sboru ČR, konkrétně na data z období 1.1. – 30.6. 2014. Tyto statistické výstupy jsou v podrobnější verzi pravidelně aktualizovány na stránkách www.hzscr.cz.

V prvním pololetí roku 2014 zasahovaly jednotky požární ochrany u **47 478 událostí,** což je o **14 %** méně než ve stejném období roku 2013. Podařilo se tak zvrátit negativní trend nárůstu incidentů, který bylo možné pozorovat od roku 2011. Ve skutečnosti byl počet hasičských výjezdů v první polovině letošního roku **vůbec nejnižší za posledních 6 let**. Nejhorším měsícem letošního roku byl květen (22,3 % zásahů), nejméně událostí se naopak stalo v únoru (12,2 %).



K nárůstu počtu událostí došlo letos pouze ve dvou krajích, Olomouckém a Zlínském. Naopak **největší pokles počtu výjezdů zaznamenal kraj Středočeský** – hasiči tu oproti minulému roku museli zasahovat **o třetinu méně**. Přes letošní pokles o 8 % si nejvyšší počet událostí s náskokem drží kraj Moravskoslezský, což je jen potvrzením fenoménu, který jsme mohli zaznamenat v předcházejících kapitolách. Naopak „nejméně práce“ mají hasiči v malých krajích – Karlovarském a Zlínském.



Nejčetnějšími událostmi byly **technické havárie – 48,5 %, následují požáry – 20,2 %, dopravní nehody – 18,1 % a úniky nebezpečných chemických látek – 5,9 %. Plané poplachy činí 7,3 % z celkového počtu událostí. Nejvíce událostí bylo v červnu** – 21,1 % z celkového počtu, nejméně v únoru – 7,0 %. Podle dnů v týdnu bylo **nejvíce** událostí v **neděli** – 16,9 % a **nejméně** v sobotu – 12,3 %.

Ačkoliv počet událostí v celkovém součtu klesl, **v případě požárů byl naopak zaznamenán nárůst o celou čtvrtinu oproti roku 2013**. Po dlouhé době tak letos **hasiči vyjížděli častěji k ohni, než k dopravním nehodám**, jejichž počet naopak klesl o 5 %. Příčinou bylo zřejmě suché počasí, neboť hořely zejména skládky, lesní porosty a přírodní prostředí vůbec. Škody při požárech nicméně oproti minulému roku klesly o 30 % na 971,4 mil. Kč.

Výši škod ovlivnily velké požáry (se škodou 1 mil. Kč a vyšší), kterých vzniklo letos 139 (-18) a přímé škody u nich dosáhly 79 % z celkových škod. Největší počet požárů je evidován ve Středočeském kraji – 1 335 (+261), nejméně v Pardubickém kraji – 321 (+34). Největší škody eviduje Středočeský kraj – 194,8 mil. Kč (+86,4), nejmenší škody eviduje kraj Karlovarský – 14,1 mil. Kč (+1,9). Nejvíce usmrcených osob při požárech bylo ve Středočeském kraji – 13 (+5), nejvíce zraněných osob je evidováno také ve Středočeském kraji – 107 (-6).

Nejčastější příčinou požáru bývá nedbalost či technická závada. Úmyslně zapáleno bylo 731 (7,6 %) z celkového počtu 9 851 požárů. 54 požárů bylo způsobeno dětmi, 15 pak vzniklo v důsledku zásahu bleskem. Příčinou 65 požárů byla dopravní nehoda.

Co se týče **dopravních nehod,** nejčetnější byly zásahy ve Středočeském kraji – 1 341 (-122), minimum v kraji Karlovarském – 251 (-3). Celkově u dopravních nehod hasiči bezprostředně zachránili či evakuovali 4 275 osob (+1 544), při zásazích se vyskytlo 322 (+44) usmrcených osob a také 6 413 (+391) zraněných osob, jimž v mnoha případech poskytli předlékařskou pomoc.

Při **únicích nebezpečných chemických látek** jsou nejčetnějšími úniky ropných produktů – 2 257 (+118), úniky plynů včetně aerosolů – 334 (-45), úniky kapalin mimo ropných produktů – 151 (+6), pevných látek – 10 (+8) a ostatních látek včetně potravinářských produktů – 50 (-8). Nejvyšší počet těchto případů byl ve Středočeském kraji – 355 (-30), nejméně v kraji Zlínském – 69 (-2).

Skupina **technické havárie** zahrnuje technické havárie – 2 (-2), následují technické pomoci – 20 110 (-9 220), technologické pomoci – 290 (-135) a ostatní pomoci – 2 620 (-498). Jsou doménou jednotek Hasičského záchranného sboru ČR jako pomoc v nouzi při otvírání uzavřených prostorů, odstraňování překážek na komunikacích, vyprošťování osob, zvířat či předmětů apod. Nejvíce případů je evidováno v kraji Moravskoslezském – 4 094 (-765), nejmenší počet v kraji Libereckém – 728 (- 180).

Zaznamenána byla i jedna radiační nehoda. Ta vznikla dne 1. dubna 2014 v areálu firmy TOMA a.s. v Otrokovicích, okr. Zlín. Při průmyslovém rentgenování svárů kovových konstrukcí budovy byla překročena hranice přírodního pozadí. Událost šetří SÚJB ve své kompetenci.

Počet **planých poplachů** se oproti loňskému období snížil o 5 %, přičemž jejich podíl na celkovém počtu událostí se zvýšil na 7,3 %. Nejčetnější (39 %) jsou plané poplachy způsobené elektrickou požární signalizací, další plané poplachy jsou způsobeny přivoláním k případu s příznakem požáru (23 %), přivolání k nenahlášenému pálení (14 %), zneužití jednotky PO (5 %) a jiné důvody (19 %). Nejvíce planých poplachů bylo v hl. m. Praze - 543 (-31), nejméně v kraji Libereckém – 131 (+20).

Hasiči bezprostředně zachránili nebo evakuovali z ohrožených prostor v letošním 1. pololetí **19 867** osob (-5 500), nejvíce při technických pomocích, dopravních nehodách a požárech. Při zásazích bylo **214** hasičů zraněno (-22), z toho 151 profesionálních (-16) a 63 dobrovolných (-6). Při zásazích se vyskytlo také **1 124** usmrcených osob (+61) – jednotky PO pomáhaly při vyprošťování a vynášení usmrcených při dopravních nehodách, požárech a při nouzovém otevírání bytů. Dále byla **9 651** zraněným osobám (+518) poskytnuta předlékařská pomoc (převážně u dopravních nehod, technických pomocí a požárů).

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. V prvním pololetí 2014 je evidováno **47 111** případů součinnosti jednotek PO s ostatními složkami (- 124). Nejvíce – 60,6 % z celkového počtu připadlo na Policii ČR, 22,5 % na zdravotnickou záchrannou službu a 8,1 % na obecní policii. Zbytek tvoří pomoci zejména místních služeb, firem, institucí, obecních úřadů a dalších.

Přehled velkých požárů se škodou 20 milionů Kč a vyšší za 1. pololetí roku 2014

1. čtvrtletí 2014

1. 1. – **Sklad a prodejna s potřebami pro hokej firmy WARRIOR SPORT spol. s.r.o.,**
Milovice – Mladá, okr. Nymburk
Příčina: zanedbání bezpečnostních předpisů.
Škoda: 23 000 000 Kč.

31. 1. – **Pekárna firmy LA LORRAINE a.s. v bývalé mrazírně,** Kladno – Kročehlavy**.**
Příčina: nedbalost při řezání ocelových konstrukcí.
Škoda: 50 000 000 Kč.
Zraněno 8 osob, zachráněny 2 osoby.

3. 3. – **Chata LIBUŠÍN,** Prostřední Bečva - Pustevny, okr. Vsetín.
Příčina: závada komínového tělesa.
Škoda: 80 500 000 Kč.

10. 3. – **Lisovna firmy GUMÁRNY a.s.,** Zubří, okr. Vsetín.
Příčina: v šetření.
Škoda: 20 000 000 Kč.

23. 3. – **Poháněcí stanice pásové dopravy firmy SEVEROČESKÉ DOLY a.s.,**
Bílina – Březánky, okr. Teplice**.**
Příčina: vznícení od zadřeného válečku pasového dopravníku.
Škoda: 25 000 000 Kč.

2. čtvrtletí 2014

20. 4. – **Galvanovna firmy KOZÁK SVITAVY spol. s.r.o.,**
Lanškroun, okr. Ústí nad Orlicí
Příčina: technická závada na připojovacím kabelu elektrické filtrace.
Škoda: 80 000 000 Kč.
Zraněni 4 hasiči, zachráněny 2 osoby.

27. 5. – **Výrobní hala a stroj na výrobu obálek firmy MEILLER GHP, spol. s. r. o,** Nýřany, okr. Plzeň sever.
Příčina: technická závada – elektrický zkrat.
Škoda: 37 000 000 Kč.

12. 6. – **Sklad výčepní a chladicí techniky firmy VARIA-PLUS, spol. s.r.o.**,
Plzeň – Litice.
Příčina: technická závada stropního zářivkového tělesa.
Škoda: 35 000 000 Kč.
Zraněn 1 hasič.

Přehled připravovaných velkých cvičení pro rok 2014

2014

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: pravděpodobně únor/březen 2015

ZDROJE 2014

- 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 2014.

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: v průběhu roku 2015.

VODA 2014

- Součinností cvičení na ověření systému nouzového zásobování vodou. Organizátorem je Ministerstvo zemědělství ČR.
- Předpokládaná doba a místo konání: 15. – 18. září 2014; Karlovy Vary

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 1. pololetí 2014

Novela nařízení vlády 432/2010 Sb.

Potřeba novelizace nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury vyplynula jak z aplikační praxe a nutnosti terminologických úprav textu, tak i z požadavku na zapracování problematiky kybernetické bezpečnosti, v souvislosti se vznikem nového zákona o kybernetické bezpečnosti.

Návrh novely toho nařízení vypracovala odborná pracovní skupina Výboru pro civilní nouzové plánování kontaktních osob resortů k řešení odborné problematiky základních funkcí státu za krizových situací a kritické infrastruktury. Změny se týkají odvětví energetiky, zdravotnictví a komunikačních a informačních systémů.

V odvětví energetiky by mělo dojít zejména ke změně limitů v oblasti výroby elektřiny a doplnění kritéria pro vedení v oblasti distribuční soustavy. Nově by měla být zahrnuta i oblast centrálního zásobování teplem. Úprava odvětví zdravotnictví je pouze terminologická a souvisí s přijetím zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování.

Nejzásadnější změna by se měla týkat odvětví komunikačních a informačních systémů, kde je navrhováno vložení oblasti kybernetické bezpečnosti, jež obsahuje kritéria pro určení informačních nebo komunikačních systémů prvkem kritické infrastruktury, podle dikce zákona o kybernetické bezpečnosti (tzv. kritická informační infrastruktura). Jsou zde uvedena jak kritéria, která jsou navázána na již určené prvky kritické infrastruktury, tak i kritéria, která nespojuje přímá vazba na již určené prvky kritické infrastruktury.

V druhé polovině roku 2014 projde návrh novely připomínkovým řízením a následně bude koncem roku předložen k projednání vládě.

Nové SOVESO III

SEVESO III - Směrnice Evropského parlamentu a Rady 2012/18/EU, o kontrole nebezpečí závažných havárií s přítomností nebezpečných látek a o změně a následném zrušení směrnice Rady 96/82/EU. Směrnice byla přijatá dne 4. července 2012 a platnost vstupuje dvacátý den od vyhlášení v Úředním věstníku Evropské unie a nahrazuje současnou směrnici Rady 96/82/ES. Je určená všem členským státům, které ji musí implementovat do 31. května 2015.

Mezi hlavní změny v SEVESU III patří:

- Přizpůsobení se změnám v systému klasifikace látek a směsí EU
  - CLP – Classification, Labellling and Packaging,
  - zavedení nových tříd a kategorii nebezpečnosti.
- Zlepšení úrovně a kvality informování veřejnosti (Aarhuská úmluva).
- Zajištění efektivnějších bezpečnostních pravidel – přísnější kontroly a podmínky.
- Cíle prevence závažných havárií a omezení následků pro lidské zdraví (zohlednit v rámci územního plánování).
- Nově do zákona o prevenci závažných havárii budou spadat provozovatelé pevninských zásobníků plynu.

V rámci SEVESO III se dále klade větší důraz na:

- Domino efekt – určení závodů, u nichž může být riziko nebo následky závažné havárie zvýšeny v důsledku zeměpisné polohy.
- Územní plánování a kontroly – dochází k detailnějšímu rozpracování. Nově definováno co je obsahem plánu kontrol.
- Bezpečnostní zpráva – zásadní změna při projednání, posouzení a schvalování bezpečnostní zprávy. Nově dochází ke zpracování posudku návrhu bezpečnostní dokumentace právnickou osobou zřízenou Ministerstvem práce a sociálních věcí.

Exkurz:
Cvičení Nákaza 2014

Ve dnech 17. – 18. 6. 2014 se uskutečnilo součinnostní cvičení Státní veterinární správy a Armády ČR s námětem „Praktická činnost v místě podezření z nebezpečné nákazy a v primárním ohnisku nebezpečné nákazy s prověřením reálnosti zpracovaného pohotovostního plánu“. Místem cvičení bylo hospodářství vojenských lesů a statků Květušín v Jihočeském kraji.

Cvičení s názvem „Nákaza 2014“ prověřilo připravenost orgánů státního veterinárního dozoru a Armády ČR na řešení mimořádných událostí. To, že je naše republika celé řady nákaz hospodářských zvířat prostá, neznamená, že spíme na vavřínech. Hlavními tématy bylo prověřit součinnost orgánů veterinární správy a veterinární služby Armády ČR v případě podezření a potvrzení nákazy slintavky a kulhavky (SLAK) v hospodářství s chovem skotu a při podezření a potvrzení afrického moru prasat (AMP) v hospodářství s prasaty a činnost krajské veterinární správy v případě podezření na AMP u divočáků.

Při cvičení byly prověřeny technické prostředky zásahových skupin Státní veterinární správy (Krizového centra) a veterinární služby Armády ČR při likvidaci ohnisek nebezpečných nákaz. Byl procvičován odběr vzorků na slintavku a kulhavku a na africký mor prasat a jejich transport na vyšetření do národní referenční laboratoře (NRL) ve Státním veterinárním ústavu v Praze (NRL pro diagnostiku SLAK) a Jihlavě (NRL pro diagnostiku AMP). Cvičení se účastnili: Vojenský veterinární ústav Hlučín (jeho zásahová skupina a skupina laboratorní diagnostiky), Státní veterinární správa a zástupci krajských veterinárních správ pro kraj Ústecký, Plzeňský, Jihočeský, Středočeský, Královéhradecký, Městské veterinární správy Praha a zástupci Ministerstva zemědělství.

Každoročně se takovéto součinnostní cvičení pořádá s cílem ověřit si nikoli „bojeschopnost“, ale schopnost řešit krizové situace. Nákazová situace v naší republice je sice dlouhodobě příznivá, ale při pohledu za hranice je jasné, že je třeba počítat se všemi riziky. Nikoli sice přímo se slintavkou a kulhavkou, byť se stále vyskytuje na hranicích EU, například v Turecku, ale třeba s africkým morem prasat, se kterým jsou stále problémy za východními hranicemi EU a několik případů bylo letos diagnostikováno i v Polsku a Lotyšsku.

Letošní cvičení prokázalo dobrou připravenost řešit možné problémy, a to jak veterinárních odborníků ze Státní veterinární správy, tak i z Armády ČR.

Exkurz:
Havárie letadla v nepřístupném terénu

Hornatý a hustě zalesněný terén podél státní hranice České a Slovenské republiky, mezi obcemi Žítková a Horná Súča, se stal v květnu dějištěm mezinárodního taktického cvičení složek integrovaného záchranného systému obou států. Jednalo o nejrozsáhlejší cvičení tohoto roku. I samotný námět cvičení, havárie letadel v nepřístupném terénu, byl v posledních letech zcela ojedinělý.

Simulovaná mimořádná událost vznikla při letovém provozu na hranici ČR a SR. Při servisním přeletu na soustředění parašutistického týmu došlo ke srážce letounu L410UVP se 16 cestujícími na palubě a 2 členy posádky s letounem CESSNA 172, který prováděl fotografický monitoring v prostoru obce Žítková.

Při pokusu o nouzové přistání se letoun roztrhnul a části jeho trupu se roztříštily v pásu téměř jednoho kilometru. V tomto úseku se nacházelo 10 cestujících ze zadní části letounu s různě vážnými poraněními, další čtyři cestující byli v šoku, dezorientovaní a zranění bloudili ve vzdálenosti několika stovek metrů od vraku.

Čtyři cestující stihli před dopadem použít dostupných padáků a vyskočit z letadla. Po dopadu však zůstali zachyceni v korunách stromů. Cestující z havarovaného letounu byli rozeseti na území po obou stranách státní hranice. Tříčlenná posádka CESSNY zůstala po střetu a následném pádu zaklíněná ve vraku letadla poblíž osady Stehlíkovo.

Účelem výcviku bylo procvičit typové činnosti zásahů a vzájemnou spolupráci všech základních složek integrovaného záchranného systému České a Slovenské republiky při havárii letounů v obtížném pohraničním terénu, se zaměřením na vyhledání a vyproštění zraněných osob a provedení přednemocniční neodkladné péče v podmínkách hromadného neštěstí. Součástí cvičení byla rovněž vzájemná spolupráce operačních a informačních středisek IZS obou republik.
Cvičení se zúčastnilo téměř 200 hasičů, policistů a záchranářů z obou států. Nasazeni byli i policejní psovodi, jízdní policisté a v pátrání pomáhal i vrtulník Policie ČR. V rolích figurantů byli připraveni určení profesionální hasiči týmu posttraumatické intervenční péče HZS Zlínského kraje, studenti Vyšší odborné školy zdravotnické ze Zlína i slovenští profesionální hasiči.

Na plánování a přípravě cvičení se podílela také řada příslušníků a zaměstnanců jednotlivých záchranných složek a vedení obou krajů. Neopomenutelnou byla i podpora ze strany Zlínského kraje.

Vybrané události ve sledovaném období

Leden

Hasiči cvičili v ostravské věznici

Ani jedenáctistupňový mráz nezabránil profesionálním hasičům (HZS MSK) ze stanice Slezská Ostrava, aby v pondělí 27. leden 2014 dopoledne absolvovali plánovaný téměř dvouhodinový výcvik v areálu ostravské Věznice Heřmanice. V jejím výrobním areálu, kde se ekologicky likvidují nejrůznější vozidla, si hasiči vyzkoušeli stříhání všech možných částí osobního automobilu Ford Mondeo pomocí hydraulických nástrojů – hlavně kvůli vyprošťování zaklíněných osob.

Věznice Heřmanice spolupracuje s Hasičským záchranným sborem Moravskoslezského kraje (HZS MSK) několik let. Hasiči tak mohli již mnohokrát trénovat v jejím areálu záchranu osob z osobních automobilů, autobusů a trolejbusů, v jednom případě se všechny tři směny (A, B, C) prostřídaly díky věznici i při výcviku na vysloužilých městských tramvajích.

Únor

Čeští hasiči pomáhali ve Slovinsku

Po třech týdnech byla 23. února 2014 ukončena humanitární mise profesionálních hasičů z Moravskoslezského kraje ve Slovinsku. Krátce po půlnoci se do Ostravy vrátilo pět profesionálních hasičů Hasičského záchranného sboru MSK a s nimi i dvě kontejnerové elektrocentrály, které zajišťovaly nouzovou výrobu elektrické energie v živelnou pohromou zasaženém Slovinsku.

Slovinsko postihlo na přelomu ledna a února 2014 husté sněžení, dešťové srážky s následnou ledovkou, lokálními povodněmi a sesuvy půdy. Tato přírodní pohroma silně poškodila místní infrastrukturu a až 10 % obyvatelstva Slovinska zůstalo bez elektrické energie.

V reakci na Slovinskou žádost o pomoc vyslala Česká republika do Slovinska humanitární misi a počátkem února odjelo šest příslušníků a jedna kontejnerová elektrocentrála 250 kVA HZS Moravskoslezského kraje. Po týdnu záchranných prací byla mise z ČR posílena o další dvě elektrocentrály, jednu 250 kVA elektrocentrálu opět poskytl HZS Moravskoslezského kraje, s třetí 500 kVA elektrocentrálou vyjeli příslušníci HZS ČR ze Záchranného útvaru Hlučín.

Ve Slovinsku se profesionální hasiči střídali v týdenních cyklech a na misi se postupně vystřídalo 17 příslušníku HZS Moravskoslezského kraje a 10 příslušníků HZS ČR ze Záchranného útvaru Hlučín. Výrobu elektrické energie ve Slovinsku zajišťovaly dvě kontejnerové elektrocentrály o výkonu 250 kVA a jedna kontejnerová elektrocentrála o výkonu 500 kVA. Společně s českými hasiči se humanitární mise ve Slovinsku účastnili i hasiči z několika dalších evropských zemí.

Nové Centrum integrovaného záchranného systému ve Frymburku

V pondělí 3. února 2014 ve 13 hodin bylo slavnostně otevřeno Centrum integrovaného záchranného systému v jihočeské obci Frymburk. Pásku slavnostně přestřihli zástupci investorů, tedy Jihočeského kraje, městyse Frymburk, Hasičského záchranného sboru České republiky a pozvaní významní hosté.

Pozvání krajského ředitele HZS Jihočeského kraje plk. Ing. Lubomíra Bureše přijali hejtman Jihočeského kraje Mgr. Jiří Zimola, první náměstkyně Mgr. Ivana Stráská, starosta městyse Frymburk

Oto Řezáč, za Generální ředitelství HZS ČR náměstek generálního ředitele plk. Ing. František Zadina, ředitel Zdravotnické záchranné služby Jihočeského kraje MUDr. Marek Slabý, starosta SH ČMS Václav Žižka. Slavnostního aktu se zúčastnili významní hosté z Generálního ředitelství HZS ČR a jím zřizovaných organizačních složek, z Ministerstva vnitra, členové vedení složek integrovaného záchranného systému, zástupci jednotky SDH městyse Frymburk, představitelé státní správy a samosprávy Jihočeského kraje a dále zástupci stavební firmy a projektové kanceláře.
V novém Centru integrovaného záchranného systému budou sloužit společně s profesionálními hasiči HZS Jihočeského kraje také záchranáři ZZS Jihočeského kraje, svá výjezdová vozidla a zázemí zde mají i dobrovolní hasiči městyse Frymburk.

Březen

Cvičné vyprošťování ze zásobníku hnědého uhlí

V trmické teplárně, která patří do Skupiny ČEZ, proběhl výcvik firemních hasičů. Ti vyprošťovali za pomoci lanové techniky zraněnou osobu ze zásobníku surového paliva (hnědého uhlí) z hloubky deseti metrů. Celá záchranná akce trvala přibližně dvacet minut a osobu se podařilo evakuovat do bezpečí. Podobná cvičení absolvuje hasičský sbor Teplárny Trmice v průběhu celého roku. Na svém kontě pak mají za loňský rok na sto dvacet ostrých výjezdů.
Hasiči z pobočné stanice požární ochrany Teplárny Trmice pracují na čtyři směny, ve 12hodinovém cyklu. Na každé směně je 1 velitel družstva, 4 strojníci a 1 dispečer. K zásahu vyjíždějí vozy s pěti hasiči.
Teplárna Trmice je součástí organizační jednotky Teplárny Hodonín, Poříčí, Tisová a Trmice v divizi výroba ČEZ, a. s. V současné době je v trmické teplárně 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 30 000 domácností a také velkou část průmyslových podniků ve svém okolí.

11. březen – 132 požárů během jediného dne

11. březen 2014 byl v hasičských statistikách mimořádný. Hasiči vyjížděli k téměř trojnásobku požárů než je dlouhodobý denní průměr - celkem jich bylo 132. Téměř polovinu z nich tvořily požáry lesního porostu a trávy. Na vině bylo především dlouhodobé sucho, které v té době v České republice panovalo.
Největším požárem dne byl požár trávy a lesního porostu po vojenských střelbách ve výcvikovém vojenském prostoru Hradiště, okres Karlovy Vary, na ploše několika desítek hektarů. Požár likvidovalo deset jednotek hasičů a nasazen byl také vrtulník letecké služby Policie ČR. Příčinou jeho vzniku byla cvičná střelba. Nikdo naštěstí nebyl zraněn.
Téměř identický případ se stal i v Jihočeském kraji, okrese Tábor. Zde po vojenských střelbách v prostoru vojenské střelnice muselo pět jednotek hasičů likvidovat požár trávy a přilehlého pole na ploše cca 25 ha. Příčinou vzniku požáru byla střelba světelnými náboji.

Hasiči lépe vybaveni proti živelním pohromám

K datu 28. února 2014 byla ukončena realizační fáze projektů operace “Zvýšení akceschopnosti Hasičského záchranného sboru České republiky pro záchranné a likvidační práce při živelních pohromách“ (ve zkratce „Živelní pohroma“).
Operace Živelní pohroma zahrnovala 13 projektů hasičských záchranných sborů krajů a 1 projekt Záchranného útvaru Hasičského záchranného sboru České republiky, které byly v letech 2012 – 2014 realizovány se spolufinancováním ze strukturálních fondů Evropské unie, konkrétně

z Integrovaného operačního programu. Celkem bylo v rámci operace Živelní pohroma pořízeno 83 kusů techniky pro Hasičský záchranný sbor České republiky a Evropská unie jejich pořízení spolufinancovala částkou 254 mil. Kč. Uvedené projekty spočívaly v pořízení generačně nové a moderní speciální techniky určené pro řešení živelních pohrom (zejména povodní a bleskových povodní). Tato technika umožňuje Hasičskému záchrannému sboru České republiky efektivnější zásah na místě mimořádné události a poskytnutím včasné a efektivní pomoci může vést ke zvýšení počtu zachráněných životů a nárůstu objemu uchráněných hodnot při mimořádné události.

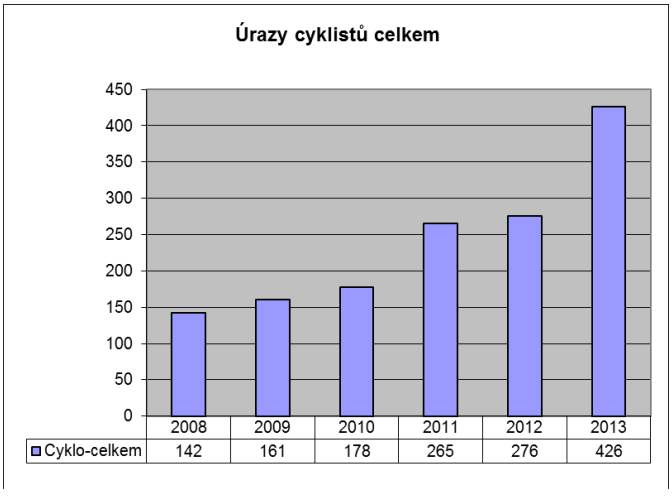
Nakoupeny byly soupravy požárního kontejnerového nosiče, požární kontejnery nákladní a nakladače; nákladní automobily pro evakuaci; technické automobily pro práci potápěčů; autobusy; požární kontejnery technické; tahač návěsů s podvalníkem; stroj univerzální; smykem řízený nakladač; automobil sklápěcí; nosič kontejnerů; automobil evakuační vyprošťovací; rypadlo pásové; jeřáb automobilní; člun nafukovací s motorem.

Duben

Cyklohlídky pražských záchranářů se osvědčily

Se stoupající oblibou cyklistiky stoupá i počet výjezdů pražských záchranářů. Zatímco v roce 2012 ošetřily posádky Zdravotnické záchranné služby hlavního města Prahy celkem 276 cyklistů, v loňském roce evidují 426 ošetřených. Tento počet představuje navýšení úrazů o 54 procent!

Ve stavu vážného ohrožení života bylo z těchto případů v roce 2012 převezeno do zdravotnických zařízení 14 pacientů. Vloni, kromě shodného počtu vážných zranění, dokonce 2 cyklisté na následky zranění zemřeli. Nejčastěji dochází ke zranění hlavy a končetin. Kromě neznalosti pravidel silničního provozu a nedostatečného používání ochranných pomůcek, patří mezi příčiny nehod i často chybějící dospělý dozor dětských cyklistů. Jejich zvyšující se počet komplikuje v metropoli hustou dopravu, vymezené trasy na cyklostezkách bývají přeplněné. Překážky bránící vjezdu vozidel však brání i vjezdu našich záchranářských posádek a tím navíc často prodlužují dojezdové časy ke zraněným.



V roce 2012 proto zařadila pražská záchranka do svého provozu zkušební záchranářskou cyklohlídku na elektrokole. Tehdy od dubna do září ošetřili záchranáři na elektrokole na cyklostezkách a v centru Prahy 35 pacientů, z toho 3 byli předáni výjezdové skupině k dalšímu ošetření a převozu do zdravotnického zařízení. Zbývajících 32 pacientů ošetřila cyklohlídka a nemusela být přivolána posádka sanitního vozu. Vloni nebyla z finančních důvodů cyklohlídka provozována.

Na základě letošní nabídky firmy Mercedes-Benz Česká republika s.r.o. využila pražská záchranka možnosti bezplatného pronájmu 2 elektrokol a od 1. května budou dva záchranáři ve 12 hodinových směnách monitorovat na elektrokolech centrum města a definované trasy cyklostezek. Stejně jako v roce 2012 budou plně vybaveni pro poskytnutí odborné první pomoci, včetně automatického externího defibrilátoru (AED).

Elektrokolo zn. Smart ebike má dojezdovou vzdálenost při podpoře šlapání 100km, dosahuje rychlosti až 25 km/h, ke 100% nabití baterie je zapotřebí 5hodin, nosnost kola je 114kg. Pohyb cyklohlídek bude sledován systémem GPS Tracker

Cvičení ERGON 2014
Dne 25. dubna 2014 v Brně - Maloměřicích proběhlo taktické cvičení k prověření koordinace složek Integrovaného záchranného systému. Simulována byla situace výbuchu plynu v objektu s množstvím zraněných. Velitel zásahu byl nucen povolat další složky IZS Jihomoravského kraje a bylo zahájeno vyprošťování osob ze sutin. Povolána byla i kynologická služba. Na místě působil i statik, střelmistři, technika pro odklízení sutin, či policejní vrtulník. Využití našel i dálkový přenos obrazu z termokamery na velitelské stanoviště, či přenos obsahu ze speciální kvadruptéry.

Květen

Cvičení úniku oleje v Dalešické přehradě
V úterý 27. 5. 2014, krátce před 17 hodinou byl zjištěn únik oleje z prasklé vysokotlaké hadice u třetího turbosoustrojí, z něhož se velká část dostala do tzv. vývaru elektrárny. Ihned po zjištění byla svolána pohotovost a událost byla nahlášena hasičům. Dvacet hasičů z jednotek HZS PS Náměšť nad Oslavou, HZS Letecké základny Náměšť nad Oslavou, JSDH Kramolín a následně také HZS PS Hrotovice zahájilo přípravu norných stěn a záchyt olejové skvrny. Samotnou likvidaci oleje komplikoval vítr a vydatný déšť, který provázel celou druhou část cvičení.

Cílem nebylo pouze ověřit činnost a připravenost hasičů, ale také připravenost obsluhy PVE Dalešice při vzniku obdobné mimořádné události a především prověřit spolupráci se zasahujícími jednotkami hasičů. Havarijní cvičení dále ověřilo funkčnost technických prostředků, prověřilo aktivaci členů Havarijního štábu provozu EDA-EMO a informování příslušných vnějších orgánů v souvislosti s mimořádnou událostí s dopadem do ekologie.

Hasiči vyrazili na elektrárnu dlouhé stráně
V pondělí 26. května 2014 vystartovali hasiči na Přečerpávací vodní elektrárnu Dlouhé Stráně. Úkol cvičení zněl – v kaverně na dně sedm metrů hluboké suché jímky se nachází pracovník s podezřením na zranění páteře. Proto na místo dorazila jednotka Hasičského záchranného sboru Olomouckého kraje ze stanice v Šumperku s lezeckou skupinou, která je předurčena pro záchranu osob z takovýchto prostor.
„Potřebovali jsme si ověřit činnosti našich zaměstnanců při vzniku mimořádné události a také spolupráci s hasiči při vyprošťování zraněných osob z těžce přístupných míst," říká Vítězslav Chmelař, který je pověřen vedením provozu elektrárny Dlouhé Stráně a doplňuje: „Současně jsme si ověřili funkčnost technických prostředků pro varování a vyrozumění zaměstnanců a osob (rozhlas, megafon, telefon), dále aktivaci členů havarijního štábu elektrárny a v neposlední řadě aktuálnost kontaktů uvedených v havarijním plánu pro informování vnějších orgánů."
„Havarijní cvičení na PVE Dlouhé Stráně bylo dalším z řady havarijních cvičení, která se každoročně konají na klasických elektrárnách a vodních elektrárnách skupiny ČEZ," říká Josef Tisoň specialista havarijní připravenosti ČEZ a vysvětluje: „Téma dnešního havarijního cvičení, záchrana těžce zraněné osoby z prostoru suché jímky jsme vybrali záměrně, neboť tato situace může při provozu elektrárny reálně nastat. Musíme být připraveni i na tento typ mimořádné události, jelikož zaměstnanci provozu elektrárny nejsou vybaveni technickými prostředky pro transport osob z těžko přístupných prostor. Havarijní cvičení je přínosné i pro členy lezecké skupiny HZS Olomouckého kraje, kteří si přímo v terénu nacvičí záchranné postupy a činnosti."

Součástí cvičení bylo i prověření alternativního způsobu otevření brány na elektrárnu při výpadku proudu pro její elektro pohon. Oba pánové se shodli, že cvičení splnilo svůj účel a určitě nebylo poslední. I když je na podrobné hodnocení cvičení ještě příliš brzy, získané poznatky nezapadnou. Hasiči i pracovníci elektrárny je přenesou do svých dokumentací. Vše se děje s velkou vážností, i když si všichni přejí, ať i další výjezdy jsou jen cvičné.

Při cvičení PORTÁL zachránili hasiči dva muže ze stožáru

Cvičení bylo zahájeno krátce po desáté hodině voláním na tísňovou linku 158. Dvě osoby uvízly na stožáru velmi vysokého napětí v Petrovicích. Když se muži (figuranti) snažili vylézt na stožár, jednomu z nich uklouzla noha a zranil se. Do 14 minut na místo přijíždí první jednotka hasičů ze Strašnic. Současně operační středisko vysílá dvě lezecké skupiny a spojuje se s pracovníky ČEPS. Přijíždí lezci z hasičské stanice Krč a Smíchov. Velení přebírá velitel čety a lezecký instruktor z hasičské stanice č. 6. Lezci zahajují zásah poté, co ČEPS potvrdila, že vedení je vypnuté a vyzkratované.
Lezci provedli výstup na stožár ke zraněným mužům, kde je zajistili proti pádu a provedli první pomoc. Velitel zásahu povolal na místo vrtulník Letecké služby PČR s hasičskými leteckými záchranáři. Zachráněný byl transportován pomocí vrtulníku a předán Zdravotnické záchranné službě a Policii ČR. Druhý figurant byl pomocí lezecké techniky s vytvořením lanovky spuštěn v nosítkách na zem, kde byl předán také ZZS a PČR.
Cvičení prověřilo dobrou spolupráci provozních pracovníků ČEPS a všech složek integrovaného záchranného systému, komunikační kanály i dojezdové časy. „Oceňuji vysokou profesionalitu zasahujících příslušníků Hasičského záchranného sboru a Letecké služby PČR“ říká Martin Bílek, bezpečnostní ředitel ČEPS, a.s.
Celá akce trvala zhruba 70 minut a cvičení se zúčastnilo na čtyři desítky cvičících.

Česká technika pomáhala v Srbsku

Ve dnech 17. – 30. května 2014 byly v Srbsku nasazeny dva odřady českých hasičů, které na místě v rámci humanitární pomoci odčerpaly ze zatopených oblastí 558 miliónů litrů vody. Srbsko bylo postiženo povodněmi stejně jako další země na Balkáně.
Spolu s odřady byla na místo dopravena a nasazena technika pořízená z Integrovaného operačního programu, konkrétně z projektu Zvýšení akceschopnosti Záchranného útvaru Hasičského záchranného sboru České republiky pro záchranné a likvidační práce při živelních pohromách. Jednalo se o nákladní automobil s nakládacím jeřábem, požární kontejnerový nosič a člun nafukovací s motorem.
Odřady hasičů byly v Srbsku vybaveny velkokapacitními čerpadly na odčerpávání vody. Člun, který si sebou hasiči přivezli, jim sloužil ke kontrole čerpadla, rovnání hadic nebo doplnění pohonných hmot do čerpadla. Velkokapacitní čerpadlo bylo při přepravě do Srbska uloženo v požárním kontejnerovém nosiči. Nákladní automobil s nakládacím jeřábem na místě sloužil také k manipulaci s čerpadly.
Projekt Zvýšení akceschopnosti Záchranného útvaru Hasičského záchranného sboru České republiky pro záchranné a likvidační práce při živelních pohromách byl spolufinancován ze strukturálních fondů Evropské unie a byl realizován v letech 2012 až 2014.

Cvičení IZS „Letecká nehoda“

Dne 5. června 2014 bylo provedeno v době od 09.00 hod. do 14.30 hod. taktické cvičení složek IZS na téma „Letecká nehoda“. Cvičení se konalo na letišti u Vyškova a jeho cílem bylo procvičit postupy dle STČ-04/IZS-Letecká nehoda, STČ-09/IZS-Mimořádná událost s velkým počtem raněných a obětí a STČ-07/IZS-Záchrana pohřešovaných osob. Z pohledu SKPV KŘP Jmk bylo dále cílem cvičení provést ohledání rozsáhlého místa mimořádné události ve spolupráci s Úřadem pro odborné zjišťování příčin leteckých nehod a DVI týmem Kriminalistického ústavu Praha. Cvičení se zúčastnilo 86 policistů, 66 hasičů a 11 zdravotníků. Za PČR se do cvičení zapojili příslušníci Územního odboru Blansko-Vyškov, výjezdové skupiny všech územních odborů PČR Jmk, Speciální pořádková jednotka KŘP Jmk, Letecká služba PP a DVI tým Kriminalistického ústavu Praha. Námětem cvičení byl pád malého dopravního letadla při přistávacím manévru a to z důvodu zhoršených klimatických podmínek. Následkem pádu letadla došlo k usmrcení 10 osob, dvě osoby byly zraněny a z místa pádu letadla se vzdálily, jedna osoba byla zraněna od trosek letadla.

V první fázi cvičení byla oblast uzavřena, provedeno dopravní opatření a dále byly zahájeny hasební práce a likvidace dalších nebezpečných úseků. Následně bylo započato s ohledáním místa události včetně identifikace obětí. Rovněž došlo k ošetření zraněné osoby a bylo zahájeno pátrání po pohřešovaných osobách. Pohřešované osoby byly vypátrány ve spolupráci s Leteckou službou PP. V rámci ohledání místa činu byly zajištěny jednotlivé stopy včetně „černých skříněk“ a byla provedena identifikace všech obětí. Rovněž byl vyzkoušen přenos obrazu z místa mimořádné události na dispečink ZZS Jmk.

Mistrovství HZS ČR ve vyprošťování

V úterý 24. června 2014 se v Amfiteátru u obchodního centra Plaza v Plzni rozhodlo o tom, který z týmů dokáže nejrychleji a hlavně nejkvalitněji poskytnout pomoc zraněným při simulované dopravní nehodě. Při VII. ročníku Mistrovství HZS České republiky ve vyprošťování zraněných osob z havarovaných vozidel se představilo 14 nejlepších družstev profesionálních hasičů z jednotlivých krajů České republiky a jedno družstvo podnikových hasičů. Úkolem čtyřčlenného týmu je bezpečně a efektivně vyprostit do patnácti minut zraněnou osobu z havarovaného vozidla. Součástí vyproštění je i poskytnutí první předlékařské pomoci a transport na místo simulující vozidlo ZZS. Pokud hasiči vyprostit osobu za stanovený časový limit nestihnou, za každých započatých 20 vteřin se jim z celkového hodnocení odečte jeden bod. Překročí-li tým 20 minut, je zásah ukončen a tým je hodnocen na konci pořadí. Pro každé družstvo je připraven jiný scénář. Všechny věrně simulují dopravní nehody, se kterými se hasiči při zásazích setkávají.

Počínání soutěžních týmů během simulovaného zásahu sleduje sbor kvalifikovaných rozhodčích z řad Hasičského záchranného sboru ČR, který hodnotí zásah a vyproštění zraněné osoby ve třech oblastech – taktika, technika provedení zásahu a poskytnutí první předlékařské pomoci zraněnému. Mezi hlavní kritéria hodnocení tedy patří v oblasti taktiky především velení u zásahu, spolupráce celého týmu, bezpečnost práce; v oblasti techniky pak ovládání vyprošťovacích zařízení, způsob využití různých ochranných prostředků na přímou ochranu zraněné osoby a vyproštění zraněného včetně zajištění životně důležitých funkcí a fixace vyprošťovaného.

Mistrovství Hasičského záchranného sboru České republiky ve vyprošťování zraněných osob z havarovaných vozidel se koná každé dva roky. Vůbec poprvé se uskutečnilo v roce 2002 v Brně, v roce 2004 jej hostily Pardubice, v roce 2006 se konalo v Praze, o dva roky později se soutěžilo v Českých Budějovicích, v roce 2010 v Přerově a poslední ročník se konal v Karlových Varech. Mistry republiky se postupně stali hasiči z Prahy, Hořovic, Boskovic, Pardubic, Prahy a opět nejúspěšnější družstvo v historii vyprošťování hasiči z Hořovic. V letošním roce uspěli pro změnu třinečtí hasiči.

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

Předpis 90/2014 Sb., **změna energetického zákona a zákona o podporovaných zdrojích energie**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=82077&fulltext=&nr=&part=&name=~2F2014&rpp=15#local-content

Předpis 111/2014 Sb., **o celkovém množství elektřiny a plynu spotřebovaném v České republice v roce 2013**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=82221&fulltext=&nr=&part=&name=~2F2014&rpp=15#local-content

Předpis 338/2014 Sb., **o dotacích ze státního rozpočtu na úhradu části ceny elektřiny**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=80742&fulltext=&nr=&part=&name=~2F2014&rpp=15#local-content

Předpis 87/2014 Sb., **změna zákona o ochraně ovzduší**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=82074&fulltext=&nr=&part=&name=~2F2014&rpp=15#local-content

Bezpečnost finančních institucí

Předpis 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

Předpis 129/2014 Sb., **o opatření proti legalizaci výnosů z trestné činnosti**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=82326&src=nove&rpp=15#local-content

Předpis 135/2014 Sb., **změna zákonů v souvislosti se stanovením přístupu k peněžním organizacím**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=82355&fulltext=&nr=&part=&name=~2F2014&rpp=15#local-content

Předpis 31/2014 Sb., **změna vyhlášky o výkonu činnosti platebních institucí**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=81737&fulltext=&nr=&part=&name=~2F2014&rpp=15#local-content

Krizové řízení

Předpis 69/2014 Sb., **o technických podmínkách věcných prostředků požární ochrany**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=81926&fulltext=&nr=&part=&name=~2F2014&rpp=15#local-content

KONFERENCE A SETKÁNÍ

Připravované akce v ČR a v SR v příštím roce

Energetika a energetická bezpečnost

1. – 3. 7. 2014 **Alternativní zdroje energie 2014**
Konference o obnovitelných zdrojích energie pro budovy zítřka
Kroměříž
http://www.azecr.cz/cz/

21. – 24. 8. 2014 **Obnovitelné zdroje energie 2014**
9. ročník výstavy
Agrokomplex Nitra, Nitra
http://www.agrokomplex.sk/vystavy/obnovitelne-zdroje-energie-2014/

10. – 12. 9. 2014 **Energetika a životní prostředí**
Mezinárodní konference týkající se velké energetiky a životního prostředí
Buly Aréna, Kravaře
http://www.vsb.cz/info/?reportId=22511

14. – 15. 10. 2014 **ElfetexFest Plzeň**
20. ročník veletrhu elektrotechniky, elektroniky a energetiky
Parkhotel Plzeň, Plzeň
http://www.omnis.cz/akce/elfetexfest-plzen-53/

14. – 17. 10. 2014 **ELOSYS**
20. ročník veletrhu elektroinženýrství, elektroniky, energetiky a telekomunikací
Expo Center Trenčín, Trenčín
http://www.expocenter.sk/ExhibitionAction.aspx?ExhibitionID=280&ItemID=131

21. – 23. 10. 2014 **Zvyšování životnosti komponent energetických zařízení v elektrárnách**
Konference hodnotící životnost energetických zařízení v elektrárnách
Srní
http://vzuplzen.cz/srni/

22. 10. 2014 **EnergoWorld 2014**
Odborná konference s doprovodnou výstavou
Kongresové centrum Vavruška, Praha
http://data.eventworld.cz/file/energoworld2014/EnergoWorld_2014_profil.pdf

6. – 8. 11. 2014 **Ekoenerga Olomouc**
15. ročník výstavy spojené s konferencí s tématikou obnovitelných zdrojů energie
Výstaviště Flora Olomouc, Olomouc
http://www.omnis.cz/akce/ekoenerga-olomouc-51/

12. – 13. 11. 2014 **ElfetexFest Ostrava**
3. ročník veletrhu elektrotechniky, elektroniky a energetiky
Multifunkční aula GONG, Ostrava
http://www.omnis.cz/akce/elfetexfest-ostrava-54/

18. 11. 2014 **ENERGO SUMMIT**
Mezinárodní konference o obnovitelných zdrojích a energetice
PVA EXPO PRAHA, Praha
http://www.energosummit.cz/2014/cz/intercept.asp

18. – 20. 11. 2014 **FOR ENERGO**
3. ročník veletrhu energetiky, elektrotechniky, elektroniky a automatizace
PVA EXPO PRAHA, Praha
http://www.forenergo.cz/2014/cz/intercept.asp

25. – 26. 11. 2014 **BIOMASA & ENERGETIKA 2014**
Mezinárodní konference o bioenergetice pořádaná Českým sdružením pro biomasu
Místo konání bude upřesněno
http://biom.cz/cz/akce/konference-biomasa-energetika-2014

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/

Bezpečnost finančních institucí

10. 6. – 11. 7. 2014 **Slovenský bankový trh 2014**
Konference o nových trendech na poli bankovnictví
Hotel Park Inn Danube, Bratislava
http://www.konference.cz/akce/detail-3033-Slovensky-bankovy-trh-2014/

23. 9. 2014 **Data Storage Workshop**
9. ročník konference o zálohování, ukládání, archivaci a správě dat
Konferenční centrum City, Praha
http://www.dsw.cz/

30. 9. 2014 **Cyber Security 2014**
Odborná konference zaměřená na kybernetickou bezpečnost
Konferenční centrum City, Praha
http://data.eventworld.cz/file/cybersecurity2014_II/CyberSecurity_2014-profil.pdf

7. 10. 2014 **Svět informatiky ve finančnictví**
4. ročník konference o novinkách v oblasti moderního bankovnictví a bezpečnosti
Konferenční centrum City, Praha
http://financnictvi.expo-net.cz/

15. – 17. 10. 2014 **Future Crises 2014**
4. ročník mezinárodní konference o kybernetické bezpečnosti pod záštitou NATO
PVA EXPO PRAHA, Praha
http://natoexhibition.org/

21. 10. 2014 **Bezpečnosť a dostupnosť dat**
6. ročník konference o komplexní ochraně informačních systémů
Hotel Crowne Plaza, Bratislava
http://bdd.exponet.sk/

6. 11. 2014 **Security Upgrade 2014**
Odborná konference věnovaná praktickým otázkám ICT bezpečnosti
Hotel Diplomat, Praha
http://www.konferenceit.cz/html/security-upgrade-2014.html

11. 11. 2014 **Cloud Computing Conference**
6. ročník konference o cloud computingu, moderní ochraně dat a bezpečnosti
Konferenční centrum City, Praha
http://www.cloudconference.cz/

12. 11. 2014 **TINF 2014**
Odborná konference o teleinformatice a elektronické komunikaci
Kongresové centrum Vavruška, Praha
http://data.eventworld.cz/file/tinf2014/profil-tinf_2014.pdf

Informační technologie a kyberbezpečnost

10. 6. 2014 **Document Management Conference**
Správa elektronických dokumentů
Praha
http://www.dmcon.cz/

18. 6. 2014 **Data & Dokumenty 2014**
Odborná konference o elektronických datech
Hotel Diplomat, Praha
http://www.konferenceit.cz/html/data-&-dokumenty-2014.html

23. 9. 2014 **Data Storage Workshop**
Produkty a služby v oblasti zálohování a bezpečné archivace.
http://www.dsw.cz/

15. – 17. 10. 2014 **Konference FUTURE CRISIS**
Konference je organizována AFCEA a Pracovní skupinou kybernetické bezpečnosti AFCEA Czech Chapter ve spolupráci se světovými odborníky na kybernetickou bezpečnost (NATO, FBI, EUROPOL).
PVA EXPO Letňany, Praha
www.natoexhibition.org

21. 10. 2014 **Bezpečnosť a dostupnosť dát**
Komplexná ochrana informačných systémov
Hotel Crowne Plaza, Bratislava
http://bdd.exponet.sk/

6. 11. 2014 **Security Upgrade 2014**
Praktické otázky ICT bezpečnosti
Hotel Diplomat, Praha
http://www.konferenceit.cz/html/security-upgrade-2014.html

12. 11. 2014 **TINF 2014**
Konference o teleinformatice
Konferenční centrum City, Praha
http://eventworld.cz/

Krizové řízení

16. – 20. 9. 2014 **Prague Fire & Security Days 2014**
6. ročník mezinárodního veletrhu nejnovějších trendů v oboru protipožární a zabezpečovací techniky, systémů a služeb
PVA EXPO PRAHA, Praha
http://www.fsdays.cz/home-cz.html

18. – 19. 9. 2014 **Krizový management 2014**
Konference o analýzách rizika a ekonomice prevence při neúplných informacích
Institut ochrany obyvatelstva, Lázně Bohdaneč
http://www.upce.cz/fes/urbv/akce-a-zajimavosti/krm2014-pozvanka.pdf

15. – 17. 10. 2014 **Future Forces 2014**
11. ročník mezinárodní výstavy pod záštitou NATO
PVA EXPO PRAHA, Praha
http://www.natoexhibition.org/

7. 11. 2014 **Pražská bezpečnostní konference**
10. ročník konference
Místo bude upřesněno
http://sbp.fsv.cuni.cz/SBP-99.html

Připravované akce v zahraničí

Energetika a energetická bezpečnost

14. – 16. 10. 2014 **World Nuclear Exhibition**
Mezinárodní veletrh jaderné energie
Paříž, Francie
http://www.world-nuclear-exhibition.com/

11. – 14. 11. 2014 **Electronica 2014**
26. ročník mezinárodního veletrhu elektronických komponent, doplňků a materiálů
Mnichov, Německo
http://www.electronica.de/

20. – 22. 11. 2014 **GET Nord**
Mezinárodní veletrh elektrického průmyslu
Hamburk, Německo
http://get-nord.de/

Bankovnictví a finanční bezpečnost

7. – 9. 10. 2014 **IT-SA**
Mezinárodní veletrh pro IT bezpečnost a ochranu
Norimberk, Německo
http://www.it-sa.de/

4. – 6. 11. 2014 **Cartes**
Světový veletrh digitálního zabezpečení, karet a identifikací
Paříž, Francie
http://www.cartes.com/

Informační technologie a kyberbezpečnost

2. - 7. 8. 2014 **Black Hat USA 2014**
Konference o kybernetické bezpečnosti a fenoménu hackingu
Mandalay Bay, Las Vegas, USA
http://www.blackhat.com/us-14

22. – 25. 9. 2014 **36th International Conference of Data Protection and Privacy Commissioners**
A New Data Protection e-World Order: Must or Myth?
Port Luis, Mauricius
http://www.privacyconference2014.org/

14. – 17. 10. 2014 **Black Hat Europe 2014**
Konference o kybernetické bezpečnosti a fenoménu hackingu
Amsterdam, Nizozemsko
http://www.blackhat.com/eu-14/

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.

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.