



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 2013

Odbor bezpečnostní politiky Ministerstva vnitra

červenec 2013

OBSAH

Úvodem.....	str. 4	
Resumé.....	str. 5	
Celková kriminalita v prvním pololetí roku 2013.....	str. 6	
Energetická bezpečnost		
Policejní a hasičské statistiky a jejich interpretace.....	str. 9	
Vybrané události za sledované období	str. 13	
Exkurz: cvičení Zóna 2013.....	str. 24	
Bezpečnost finančních institucí		
Policejní statistiky a jejich interpretace.....	str. 26	
Exkurz: Fenomén skimmingu.....	str. 30	
Vybrané události za sledované období.....	str. 32	
Informační technologie a kybernetická bezpečnost		
Policejní statistiky a jejich interpretace.....	str. 39	
Očekávané bezpečnostní hrozby a trendy pro rok 2013.....	str. 41	
Exkurz: Březnové hackerské útoky.....	str. 43	
Vybrané události za sledované období.....	str. 45	
Krizové řízení		
Statistiky a jejich interpretace.....	str. 53	
Přehled připravovaných cvičení krizového řízení pro léta 2013 a 2014.....	str. 61	
Exkurz: Pokračování kauzy metylalkohol v ČR.....	str. 64	
Exkurz: Povodně 2013.....	str. 65	
Vybrané události za sledované období.....	str. 73	
Novinky v legislativě ČR za sledované období		
Energetická bezpečnost.....	str. 80	
Informační technologie a kybernetická bezpečnost.....	str. 80	
Krizové řízení.....	str. 80	
Konference a setkání		
Připravované akce v ČR a SR.....	str. 81	
Připravované akce v zahraničí.....	str. 83	
Použité zdroje.....	str. 84	

ÚVODEM

Vážení čtenáři,

dostává se Vám do rukou periodická situační zpráva, která mapuje vybrané oblasti bezpečnosti v prvním pololetí roku 2013. 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 projeví 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 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 energetické bezpečnosti je tak zvláštní oddíl věnován souhrnné informaci o cvičení Zóna 2013, jež proběhlo na jaderné elektrárně Dukovany v březnu letošního roku.

V sekci o kybernetické bezpečnosti a informační kriminalitě čtenář nalezne oddíl věnující se kybernetickým útokům, jimž čelily zpravodajské servery a sekce internetového bankovníctví několika českých bank a spořitelen v březnu letošního roku. Kapitola o krizovém řízení je pak rozšířena o přehled připravovaných velkých cvičení v letošním a příštím roce, přičemž blíže bude představeno cvičení Restart 2013. V rámci sekce krizového řízení budou také přehledně shrnuty červnové povodně a stručná informace bude věnována také pokračování kauzy Metyl.

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 2013. Z ní vyplývá, že Policie ČR registrovala celkem 167 526 trestných činů, což je nárůst o 6,7% oproti stejnému období předchozího roku. Nepatrně se také snížila objasňenost trestných činů a to o 0,7%. Ve sledovaném období klesla pouze násilná kriminalita, kriminalita mravnostní, majetková, hospodářská a ostatní vzrostly (např. hospodářská kriminalita o více než 11%). Zjištěné škody poklesly o 10,6%.

Z údajů policie zaměřených na energetický sektor je možné učinit závěr, že v ČR nedochází k téměř žádným cíleným útokům na energetickou infrastrukturu. Největší problémy způsobují především krádeže a podvody různého rozsahu. Nejvyšší škody mají na svědomí zloději kabelů, vodičů, elektroinstalačního materiálu a dalších zpeněžitelných položek. Klíčovými událostmi v oblasti energetické bezpečnosti byly červené požáry trafostanic v Praze. V rámci sekce vybraných událostí je také pozornost věnována výbuchu budovy v Divadelní ulici v Praze v dubnu letošního roku.

Nejvýznamnější událostí bylo bezpochyby cvičení Zóna 2013, které proběhlo v jaderné elektrárně Dukovany a jehož cílem bylo simulovat „black-out“.

Kapitola o bezpečnosti finančních institucí prezentuje statistiky kriminality cílené na toto odvětví, které trápí především různé formy podvodného jednání. Výše škod dosáhla v součtu za první pololetí roku 2013 více než jedné miliardy a 147 milionů korun. Blíže je představen fenomén skimmingu, jenž se letos v několika desítkách případů objevil také v ČR. V letošním roce je patrný přesun tohoto fenoménu z Prahy do dalších měst po celé republice.

Z údajů policie o problematice informační kriminality lze vyčíst, že trend kybernetického zločinu je nadále na vzestupu. Oproti prvnímu pololetí loňského roku došlo ke zvýšení o více než 400 případů. V rámci exkurzu je prostor věnován březnovým hackerským útokům, jimž čelily nejprve zpravodajské weby, poté portál Seznam.cz, následně weby několika velkých bank a poté weby mobilních operátorů. Hackerské útoky byly v prvním pololetí letošního roku aktuální také v zahraničí, čelily jim mimo jiné také komunikační platformy Twitter a Facebook. Závěr měsíce června se pak nesl ve znamení kauzy Edwarda Snowdena a aféry Prism.

V kapitole o krizovém řízení je největší prostor věnován exkurzu o červnových povodních. Jsou zde ale také představeny statistiky za rok 2012 a za první čtvrtletí roku 2013. Co se požárů týče, klesl jejich počet za první čtvrtletí o 12%.

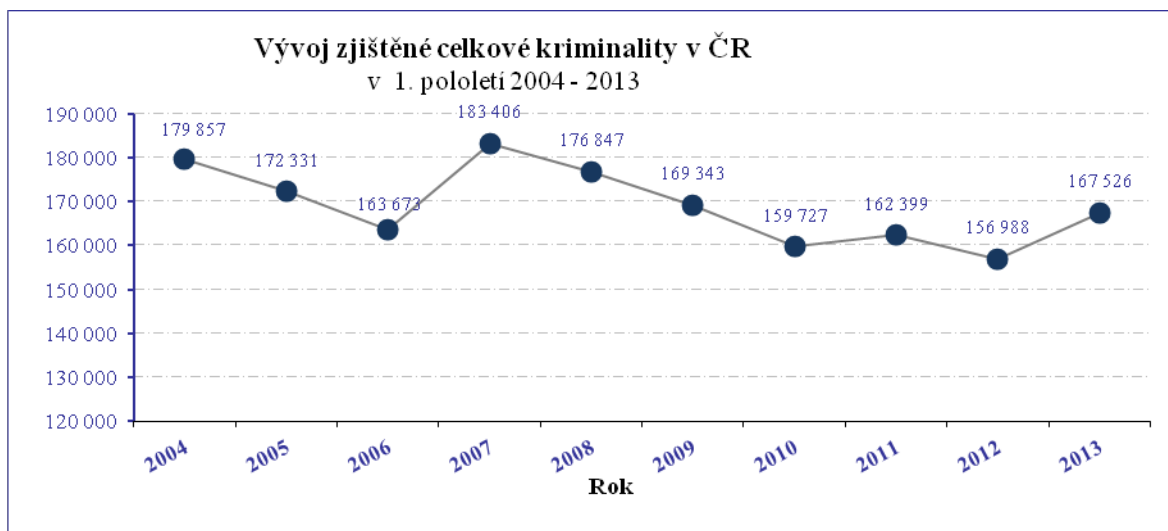
Důležitou událostí budou podzimní cvičení Restart 2013, které bude simulovat lokální „black-out“ Pardubického a Královéhradeckého kraje, a cvičení Blaník 2013, jehož tématem je ohrožení bezpečnosti civilního letectví.

Poslední dvě kapitoly poukazují na některé legislativní změny, které ve zkoumaných oblastech proběhly a naleznete zde také odkazy na řadu konferencí a akcí věnovaných bezpečnosti zmiňovaných sektorů.

CELKOVÁ KRIMINALITA V ČR V PRVNÍM POLOLETÍ ROKU 2013

Registrovaná kriminalita v meziročním srovnání

Za období od 1. 1. do 30. 6. 2013 Policie ČR registrovala celkem 167 526 trestných činů (+10 538, +6,7 %). Ačkoliv meziroční nárůst zjištěné kriminality je již poměrně znepokojivý, absolutní počet zjištěných trestných činů je stále pod desetiletým průměrem (od roku 2004), který přesahuje hranici 169 000 skutků. Vývoj zjištěné kriminality za srovnatelná období za posledních 10 let znázorňuje níže uvedený graf.



Zdroj: PCR

Objasněno bylo 60 966 skutků (+2 808, +4,8 %). Počet objasněných trestných činů zůstal rovněž pod desetiletým průměrem (od r. 2004), který přesahuje hodnotu 62 540 skutků.

Celková objasněnost dosáhla 36,4 % a meziročně se snížila o 0,7 %

Zjištěné hmotné škody meziročně **poklesly**, a to o téměř 10,6 % na cca **16 mld. Kč** (v pololetí roku 2012 cca 17,9 mld.).

Nejvyšší škody byly způsobeny trestnými činy: krácení daně, podvod a porušování povinností při správě cizího majetku.

Zjištěná kriminalita meziročně vzrostla o 6,7%
Počet objasněných trestných činů vzrostl o 4,8%

Počty zjištěných trestných činů ve většině hlavních kategorií kriminality vzrostly:

- mravnostní kriminalita (+1,1 %)
- majetková kriminalita (+8,1 %)
- ostatní kriminalita (+10,9 %)
- hospodářská kriminalita (+11,3 %)

Poklesla pouze

- násilná kriminalita (-2,1 %)

Zjištěné škody poklesly o 10,6%, zajištěné hodnoty¹ vzrostly o cca 24%.

Zdroj: PČR

Vybrané markanty registrované kriminality

Významně vzrostly krádeže vloupáním celkem (+ 4737, +16,8%).

V absolutních číslech **nejvíce vzrostl počet krádeží vloupáním do ostatních objektů²** (+2 534, +14,9 %), jimiž také byly v rámci obecné kriminality způsobeny největší škody.

Druhý nejvyšší nárůst byl zaznamenán u krádeží věcí z aut (+1 548, +11 %). Následují úvěrové podvody.

Krádeže vloupáním do rodinných domků vzrostly meziročně o 857 skutků, tj. o 33,2 %

Největší meziroční poklesy v absolutních číslech byly zaznamenány u trestných činů: nedbalostní dopravní nehody silniční, krádeže ostatní, ochrana měny a také **loupeže (-184, -10,5 %)**.

V rámci násilné kriminality poklesl rovněž počet **úmyslných ublížení na zdraví (-137, -4,8 %)**.

Stíhané a vyšetřované osoby

Celkem bylo v prvním pololetí tohoto roku stíháno a vyšetřováno 59 953 osob. Meziroční vývoj je patrný z tabulky.

Meziročně došlo k nárůstu počtu stíhaných a vyšetřovaných osob (+592 osob, + 1 %).

	2012	tj. %	2013	tj. %
Celkem osob	59 361	100,0	59 953	100,0
recidivisté	29 732	50,1	31 275	52,2
nezletilí do 15 let	714	1,2	639	1,1
mladiství 15 až 18 let	1 883	3,2	1 509	2,5
ženy	8 073	13,6	8 411	14,0
cizinci	3 955	6,7	3 818	6,4

Zdroj: PČR

¹ Tzv. „zajištěné hodnoty“ (na místě činu nebo v časovém sledu krátce poté) je třeba odlišovat od **výnosů z trestné činnosti zabavovaných v průběhu trestního řízení, kde naopak dochází k pozitivnímu vývoji.**

² Což je druh krádeží dle policejní takticko-statistické klasifikace (TSK), kdy objektem napadení jsou např. sklepy, garáže, dílny, stodoly a kůlny, zahradní altány, dvory a zahrady aj. Policejní klasifikace je v tomto ohledu podrobnější než klasifikace trestního zákoníku, člení krádeže dle § 205 tr. zákoníku podle dalších taktických hledisek.

Z tabulky 1 vyplývá další meziroční nárůst počtu recidivistů (+1543, +5,2 %), který je již dlouhodobým trendem. Celkový podíl recidivistů na stíhaných a vyšetřovaných osobách dosáhl rekordní hranice 52,2 %.

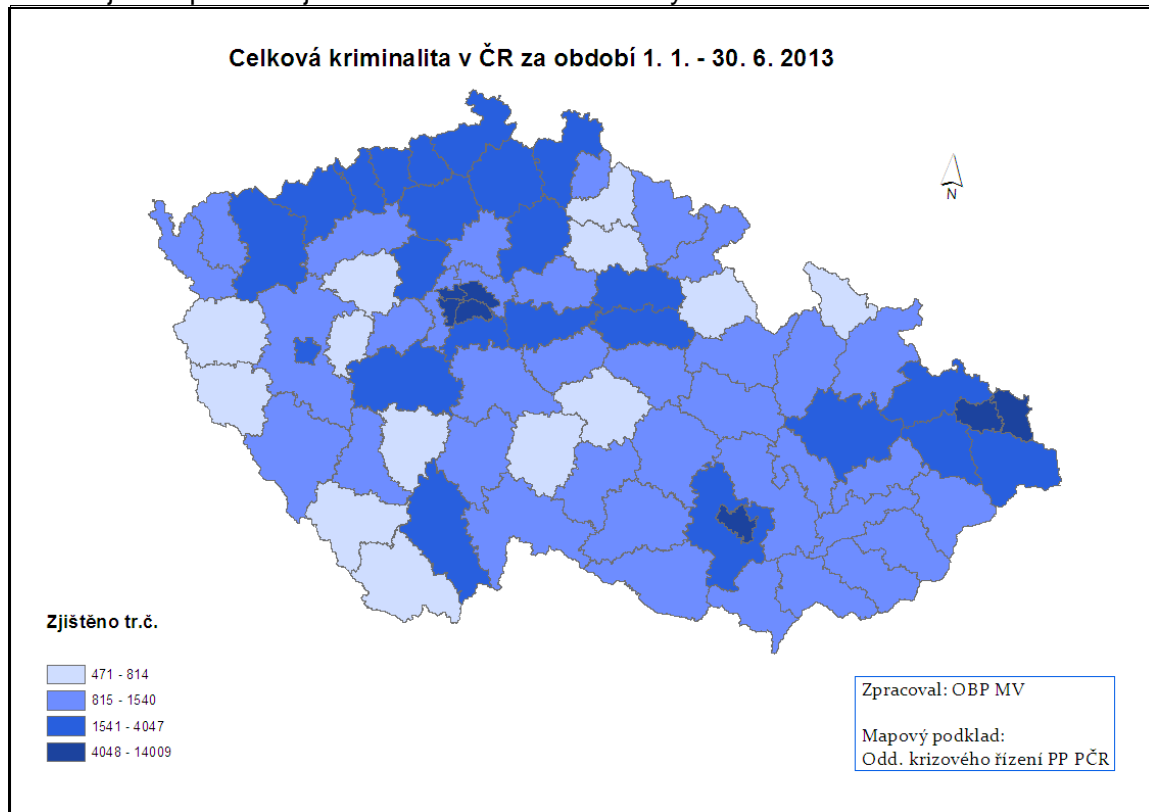
Recidivisté spáchali za sledované období 45 vražd, tj. 51,7 % ze všech spáchaných vražd.

V následující tabulce je uveden celkový počet stíhaných osob za roky 2011 a 2012.

	2011	tj. %	2012	tj. %
Celkem osob	114 975	100,0	113 026	100
recidivisté	55 717	48,5	56 489	50
nezletilí do 15 let mladiství 15 až 18 let	1 568	1,4	1 371	1,2
ženy	4038	3,5	3 486	3,1
zizinci	15 260	13,3	15 479	13,7
	7 473	6,5	7 513	6,6

Zdroj: PČR

Následující mapa ukazuje rozložení celkové kriminality v ČR dle územních odborů Policie ČR.



Další informace a statistiky naleznete v souhrnné „**Zprávě o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2013**“, kterou zpracovává odbor bezpečnostní politiky a naleznete ji na jaře příštího roku na stránkách Ministerstva vnitra www.mvcr.cz. „Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2012“ je již na stránkách Ministerstva vnitra dostupná.³

³ Zpráva je dostupná na internetové adrese <http://www.mvcr.cz/clanek/zprava-o-situaci-v-oblasti-vnitri-bezpecnosti-a-verejneho-poradku-na-uzemi-cr-v-roce-2012.aspx>

ENERGETICKÁ BEZPEČNOST



Policejní statistiky a jejich interpretace

Trestné činy za období 1. 1. – 30. 6. 2013 dle „druhu napadených objektů“

druh objektu	zjištěno tr. činů	škody
trafostanice a rozvody elektrického proudu	594	38 640 300 Kč
plynárny	115	5 138 100 Kč
elektrárny	190	14 088 900 Kč
teplárny	37	2 551 100 Kč
energetické závody	392	25 758 600 Kč
tranzitní plynovody	2	25 500 Kč
tranzitní ropovody	1	45 000 Kč
celkový součet	1331	86 247 500 Kč

Zdroj: PCR

Z uvedených statistik trestné činnosti za první pololetí roku 2013 vyplývá, že ve výše zmíněných objektech energetické infrastruktury došlo celkem k více než třinácti stům trestných činů, přičemž škody z nich přesáhly částku osmdesáti milionů korun. Došlo tak ke zvýšení počtu trestných činů oproti údajům od 1.1.2012 do 30.9.2012, kdy bylo zjištěno 1090 trestných činů. Naopak došlo ke snížení rozsahu škod, jenž ve výše uvedeném období od 1.1.2012 do 30.9.2012 dosáhl téměř 110,5 milionu Kč.

Tato na první pohled poněkud alarmující čísla je ovšem nutné správně interpretovat. **V naprosté většině případů šlo totiž o „běžnou“ kriminalitu, především o krádeže a podvody různého rozsahu.** V kontextu této situační zprávy je nutné zdůraznit, že žádný teroristický útok, který by měl za cíl narušit energetickou infrastrukturu v ČR, se ve sledovaném období nestal.

Pokud se tedy podíváme blíže na výše uvedenou tabulku a kromě „druhu napadeného objektu“ se zaměříme rovněž na „předmět zájmu pachatele“, zjistíme, že **největší množství případů i výši škod mají na svědomí zloději kabelů, vodičů, elektroinstalačního materiálu a dalších zpeněžitelných položek, dále se pak jednalo o krádeže elektrické či tepelné energie a o podvody při jejím využívání.** Ve zhruba čtvrtině případů se pak podařilo zjistit pachatele.

Hasičské statistiky a jejich interpretace

O nehodách a souvisejících škodách nám více než policejní zdroje poslouží statistiky vedené MV - Generálním ředitelstvím Hasičského záchranného sboru ČR. Aktuálně je k dispozici souhrn dat za první čtvrtletí tohoto roku a přehled dat za uplynulý rok 2012. Údaje za druhé čtvrtletí se teprve zpracovávají. Statistické informace od HZS jsou šířeji pojednány ve 4. kapitole této situační zprávy, která je věnována krizovému řízení. V této části se blíže zaměříme pouze na údaje, jež mají vazbu k energetické infrastruktuře. Na základě informací uvedených v souhrnu dat za první

čtvrtletí tohoto roku nedošlo v prvních třech měsících k požárům v energetických odvětvích v hospodářství.

V období od 1. 1. do 31. 3. 2013 vzniklo v ČR **3 798** požárů (s účastí i bez účasti jednotek PO). Přímé škody dosáhly částky **596,8** mil. Kč, **44** osob bylo usmrceno a dalších **351** osob zraněno.

Počet požárů je letos oproti stejnému období loňského roku nižší o 39,5 %, škody jsou vyšší o 8,4 %. Počet usmrcených osob je nižší o 14 % a počet zraněných nižší o 10 %. Jednotky PO uchránily před zničením hodnoty za **4 570,0** mil. Kč.

Požáry v energetických odvětvích hospodářství v ČR od 1. ledna do 31. prosince 2012

odvětví	počet požárů	podíl v %	škody v Kč	usmrcených	zraněných
energetické výrobní budovy	85		162 859 300	1	2
výroba, rozvod el. a plynu	167	0,81	164 518 700	0	11

Zdroj: MV-GR HZS ČR

V roce 2012 vzniklo v České republice celkem 19 908 požárů. Pouhých 0,8% se týkalo výroby a rozvodu elektřiny a plynu, případně těžby nerostných surovin. Škody v těchto dvou odvětvích přesáhly 160 milionů korun, zraněno bylo celkem 11 osob.

Následující tabulka shrnuje požáry (včetně výbuchů na bázi hoření) v odvětví výroby a rozvodu elektřiny, plynu a vody za poslední tři roky. Změny v jednotlivých letech jsou zaznamenány v grafu na následující straně.

rok období	2010		2011		2012	
	počet	škoda mil.Kč	počet	škoda mil.Kč	počet	škoda mil.Kč
1. Q	30	6,2	39	11,8	29	4,4
2. Q	39	44,7	48	19,1	52	18
3. Q	55	20,3	42	6,2	54	125,5
4. Q	33	4,4	36	1,9	32	16,6
celkem	157	75,4	165	39	167	164,5

Zdroj: MV-GR HZS ČR

Tabulka 1 shrnuje požáry včetně výbuchů na bázi hoření v odvětví výroby a rozvodu elektřiny, plynu a vody za první dvě čtvrtletí roku 2013. Celkově se jedná o 89 případů dosahujících škody 237,3 milionu korun. Tabulka 2 shrnuje požáry včetně výbuchů na bázi hoření v energetických budovách. Celkově se jedná o 54 případů a škody 134,4 milionu korun.

Tabulka 1

rok období	2013	
	počet	škoda mil. Kč
1.Q	34	7,6
2.Q	55	229,7
celkem	89	237,3

Tabulka 2

rok	2013	
období	počet	škoda mil. Kč
1.Q	26	4,2
2.Q	28	130,2
celkem	54	134,4

Zdroj: MV-GŘ HZS ČR

Výčet velkých požárů ve druhé polovině roku 2012, jejichž škoda přesáhla 10 milionů korun, je uveden níže.

Rok 2012 (červenec-prosinec)

20. 7. • Hala odvodnění energosádrovce bývalého objektu odsíření ELEKTRÁRNA TUŠIMICE – ČEZ, a.s., Tušimice, okr. Chomutov.

Příčina: nedbalost při svařování.

Škoda: 100 000 000 Kč.

25. 8. • Průmyslový sklad se střešní fotovoltaickou elektrárnou firmy SOUTH POINT DCC spol. s r.o., Kunice, okr. Praha-východ.

Příčina: elektrický zkrat diodového můstku v rozvodné desce elektrárny.

Škoda: 17 000 000 Kč.

19. 9. • Elektrická rozvodna TEPLÁRNA TRMICE, a.s., Ústí nad Labem-Trmice.

Příčina: elektrický zkrat zařízení rozvodny v důsledku kontaktu s vodou unikající poškozeným těsněním.

Škoda: 19 000 000 Kč.

12. 10. • Sportovní hala SPORT EDEN, o.s., Beroun.

Příčina: elektrický zkrat fotovoltaického panelu.

Škoda: 15 000 000 Kč.

31. 10. • Transformátor fotovoltaické elektrárny firmy WIS ENERGO LEDCE SEVER, spol. s r.o., Ledce, okr. Brno-venkov.

Příčina: nepředpokládané změny provozních parametrů.

Škoda: 11 600 000 Kč.

Rok 2013 (leden – červen)

27.2.2013 - požár trafostanice v Litvli (Nasobůrky)

Žádná zranění

Škoda: 2 000 000 Kč

10.6.2013 - trafostanice firmy TŽ a.s., Třinec, okr. Frýdek-Místek

Technická závada – elektrický zkrat na odpojovači fáze

Škoda: 22 000 000 Kč

18.6.2013 - trafostanice firmy ČEPS a.s., Praha – Kunratice, část Šeberov

Technická závada

Škoda: 100 000 000 Kč

Zdroj: MV-GŘ HZS ČR, idnes.cz, ceeps.cz

Do hasičských statistik se kromě požárů pochopitelně dostaly i technické havárie a úniky nebezpečných látek (včetně ropy a plynu), ty nicméně nejsou členěny podle zasaženého odvětví. Podrobné údaje je možné nalézt na internetových stránkách MV-GŘ HZS ČR, ve stručnější souhrnné podobě pak v kapitole této zprávy, věnované krizovému řízení.

Odkazy na důležité strategické dokumenty

Aktualizovaná Státní energetická koncepce 2012

<http://download.mpo.cz/get/47607/53721/595041/priloha001.pdf>

Národní akční plán České republiky pro energii z obnovitelných zdrojů

<http://www.mpo.cz/assets/cz/2012/11/NAP.pdf>

Návrh aktualizované Surovinové politiky ČR

<http://download.mpo.cz/get/46609/52547/591227/priloha002.pdf>

+ přílohová část

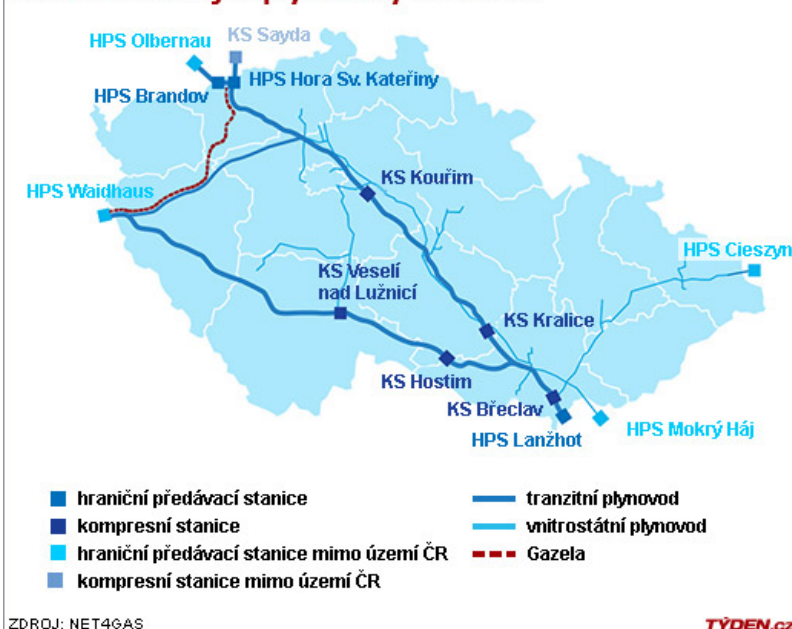
<http://download.mpo.cz/get/46609/52547/591228/priloha001.pdf>

Leden

Provoz 166 km dlouhého plynovodu Gazela byl zahájen

Premiér Petr Nečas zahájil spolu se zástupci Německa a Ruska provoz 166 kilometrů dlouhého plynovodu Gazela. Vysokotlaká linie, jež vede po trase z Mostecka na Tachovsko, napojila ČR na zemní plyn z nových ruských zdrojů, který do Evropy proudí plynovodem Nord Stream vedeným po dně Baltského moře. Rourami o průměru 1,4 metru ročně proteče až 30 miliard metrů krychlových plynu, což je tak 3,5násobek spotřeby ČR. ČTK to řekl Radek Benčík, jednatel NET4GAS, investora největší současné energetické stavby v ČR za deset miliard korun. Její návratnost by měla být desetiletá.

Gazela a stávající plynovody NET4GAS



Stavba zakončila obří rusko-německý projekt Nord Stream. Gazela, která také spojí plynovody Opal na severu Německa a Megal na jihu, je na čtyřech místech propojena s českou přepravní soustavou a má strategickou roli v případě přerušení dodávek plynu z Ruska přes Ukrajinu, což se stalo v roce 2009, a také přes Bělorusko. 'Jde o úplně novou trasu s velkou kapacitou, která se stane trasou hlavní. Nyní už se pro dopravu plynu do Česka z větší části využívá Opal než tranzit ze Slovenska,' uvedl manažer projektu Pavel Nesládek. Soustava plynovodů může dodávat plyn oběma směry, tedy z Německa do i z ČR a na Slovensko.

'Gazela zvyšuje velmi výrazným způsobem energetickou bezpečnost naší země i našich partnerů v EU. Je to významný mezinárodní projekt, protože umožňuje zásobovat i jižní Německo a další regiony Evropy,' řekl Nečas. Podle něj se ukazuje, že propojování energetických sítí a dopravních tras je v rámci EU perspektivní a důležité, protože zvyšuje konkurenceschopnost a umožňuje diverzifikovat zdroje i přepravní trasy. Podle něj potřebuje mít ČR jako průmyslová země i 'rozumné ceny energií včetně zemního plynu'.

Gazela, kterou proudí plyn od konce loňského roku, bude z hlediska objemu dodávek jedna z nejdůležitějších a nejvíce zatížených. ČR se tak stává velkou křižovatkou dopravy plynu v Evropě, jelikož je schopná transportu z východu na západ i ze severu na jih.

Gazela, jejíž stavba byla zahájena předloni v říjnu, začíná v Brandově na Mostecku a končí v Přimdě na Tachovsku. V Plzeňském kraji měří téměř 90 kilometrů. Třetinu stavby, většinou v Ústeckém kraji, stavěl český Plynostav a ruský Strojtransgaz, zbytek belgicko-rakouské konsorcium Denys-Alpin. Gazela kříží 66 silnic, 13 železnic a 51 toků.

Nejsložitější bylo podle Nesládky tříleté jednání s 1035 vlastníky asi 3000 pozemků. Museli souhlasit s vedením pod zemí a umožnit přístup, pokud by se na linii něco stalo. Desítky pozemků musel NET4GAS vykoupit. Šlo o plochy pod trasovými uzávěry rozloženými po 20 kilometrech a pozemky, jejichž majitel neuzavřel smlouvu o věcném břemenu.

ČEZ schválil upravenou dohodu o narovnání s Evropskou komisí, kterou se zavazuje prodat jednu z elektráren Počerady, Chvaletice nebo společně elektrárny Tisová a Mělník 3

Představenstvo a dozorčí rada ČEZ dnes schválily upravenou dohodu o narovnání s Evropskou komisí, která znamená zásadní krok k ukončení šetření vedeného Evropskou komisí od roku 2009 vůči ČEZ. ČEZ již v červnu loňského roku nabídl EK, že ukončí šetření této formou, a to konkrétně závazkem prodat některou z elektráren Počerady, Chvaletice, Dětmárovice nebo Tisová spolu s Mělníkem 3. Ve všech případech se jedná o elektrárny, kde ČEZ neplánuje zásadní rekonstrukce, ale postupný útlum v závislosti dosažení konce technické životnosti jednotlivých zařízení. Upravená dohoda již neobsahuje elektrárnu Dětmárovice. Tato dohoda nabyde platnosti po schválení Evropskou komisí.

Velká havárie jaderné elektrárny by Francii přišla na pětinu HDP

Případná velká havárie jaderné elektrárny podobná havárii v japonské Fukušimě by Francii stála 430 miliard eur (10,9 bilionu korun), tedy asi 20 procent jejího hrubého domácího produktu (HDP). Vyplývá to z dnes zveřejněné studie státního institutu pro jadernou bezpečnost IRSN.

Velká havárie na jednom z 58 francouzských jaderných reaktorů by zamořila životní prostředí, vyhnala z domovů 100.000 lidí, zničila zemědělské plodiny a způsobila velké výpadky dodávek elektřiny. 'Velká nehoda by měla hrozné důsledky, ale museli bychom se s nimi vyrovnat a musíme o tom mluvit,' řekl šéf IRSN Jacques Repussard.

Velké finanční ztráty by způsobily také škody na pověsti země. Jaderná katastrofa by postihla vývoz francouzských potravin a lahůdek a turistický průmysl. Tyto škody by dosáhly 160 miliard eur. Pokles turistiky by zasáhl nejen postiženou oblast, ale celou Francii, řekl vedoucí studie Patrick Momal. Zdůraznil, že i kdyby francouzská vína a další zemědělské produkty nebyly zamořeny, jejich vývoz by prudce poklesl.

IRSN odhaduje, že katastrofa ve Fukušimě přišla Japonsko asi na 200 miliard eur. I když jsou to ohromné náklady, jsou menší, než jakým by čelila Francie - především kvůli velikosti turistického průmyslu.

Studie připravila dva katastrofické scénáře pro typický francouzský reaktor s výkonem 900 megawattů. 'Vážná' nehoda šestého stupně na sedmibodové škále INES používané Mezinárodní agenturou pro atomovou energii by stála Francii 120 miliard eur, tedy asi šest procent HDP. Například havárie v americké jaderné elektrárně Three Mile Island v roce 1979 byla na stupni pět. Její důsledky, včetně 10.000 lidí vyhnaných z domovů, by byly 'zvládnutelné', uvedla IRSN.

'Velká' nehoda na stupni sedm odpovídající haváriím v Černobylu nebo Fukušimě by však znamenala pro Francii 'katastrofu' a 'silně a trvale by zemi traumatizovala', píše zpráva. Podle ní by uvolněný radioaktivní materiál měl vážné zdravotní důsledky, zamoření půdy by bylo dlouhodobé a byly by zasaženy i sousední země.

'Musíme mít na paměti, že pravděpodobnost takových nehod zůstává mimořádně nízká,' řekl Momal. 'Ale tyto odhady pomáhají politikům dostat do patřičné perspektivy náklady na preventivní opatření.'

Je to první státní studie tohoto druhu ve Francii, která ze všech zemí světa nejvíc spoléhá na jadernou energii. Všechny 58 reaktorů provozuje státní elektrárenská společnost EDF. Po pohromě ve Fukušimě francouzský regulační úřad vyzval EDF, aby své elektrárny modernizovala. Podle EDF to bude stát asi deset miliard eur.

Francouzský prezident François Hollande chce snížit podíl jaderné energetiky na výrobě elektřiny z nynějších 75 na 50 procent v roce 2025. K nejhorší nehodě ve Francii došlo v jaderné elektrárně Saint-Laurent-des-Eaux v roce 1980, která dosáhla stupně čtyři na stupnici INES.

Reforma německé energetiky by mohla stát až bilion eur

Náklady na reformu německého energetického sektoru by se mohly vyšplhat až na bilion eur (25 bilionů Kč). Uvedl to německý ministr životního prostředí Peter Altmaier. Německo se předloni rozhodlo opustit jadernou energii a v rámci nové strategie 'Energiewende' se soustředí na obnovitelné zdroje.

'Náklady na naši energetickou reformu a restrukturalizaci dodávek energie by mohly do konce třicátých let tohoto století dosáhnout miliardy eur,' řekl ministr v rozhovoru pro německý list Frankfurter Allgemeine Zeitung. Náklady by nicméně mohlo snížit omezení dotací pro producenty energie z obnovitelných zdrojů, napsala agentura Reuters.

Ministr uvedl, že vláda se v březnu pokusí se spolkovými zeměmi dohodnout na plánech na omezení růstu cen energie. Podle analytiků investiční banky Macquarie německému trhu s elektřinou uškodila silná podpora obnovitelných zdrojů, která jde proti zájmu spotřebitelů. Maloobchodní ceny se budou podle analytiků dál zvyšovat, aby pokryly náklady na výstavbu solárních a větrných elektráren a jejich připojování do sítě.

Německo v březnu 2011 v reakci na havárii japonské jaderné elektrárny Fukušima vyřadilo na tři měsíce z provozu sedm jaderných reaktorů postavených před rokem 1980. Později německá vládní koalice rozhodla, že tyto elektrárny spolu s poruchovým reaktorem v Krümmelu již nebudou znovu uvedeny do provozu a zbývající jaderná zařízení v zemi budou odstavena nejpozději do roku 2022.

Na Olomoucku vyhořela trafostanice, škoda dosáhla dvou milionů

Škodu dva miliony korun způsobil požár, který zasáhl v noci na dnešek trafostanici v části Litovle v Nasobůrkách na Olomoucku. Oheň na místě likvidovalo několik jednotek hasičů, požár se jim podařilo dostat vzápětí pod kontrolu. Jeho příčina se vyšetřuje.

'Požár se hasičům podařilo dostat pod kontrolu zhruba po hodině od ohlášení události, následně po celkové likvidaci prostory odvětrali a vyčkali příjezdu hotovostní služby energetiků. Při požáru nedošlo k žádnému zranění,' uvedl mluvčí hasičů. Na místě zasahovali hasiči z Litovle s velkokapacitním zařízením pro hašení zařízení pod proudem, posílení o další dvě jednotky dobrovolných hasičů.

Podle mluvčího skupiny ČEZ pro střední a severní Moravu Jaroslava Jurči oheň zasáhl rozvodnu v litovelské průmyslové zóně, která společnosti nepatřila. 'Způsobil v noci výpadek elektřiny od 22:06 do 00:30, zasáhlo to 20 distribučních trafostanic,' řekl ČTK Jurča.

Březen

Politici ve východní Evropě říkají jaderné energii dál ano

I po nehodě reaktoru v japonské jaderné elektrárně Fukušima politici v Polsku, Pobaltí, v Česku a na Slovensku nadále trvají na svých plánech s atomovou energií. Navzdory výrazné nelibosti obyvatel, píše agentura DPA.

Litevci vyjádřili jasný postoj v referendu z října 2012. Téměř 63 procent oprávněných voličů se vyslovilo proti výstavbě jaderné elektrárny ve městě Visaginas. To ale vůbec nic nezmění na atomových plánech vlády ve Vilniusu - referendum není právně závazné. Do roku 2022 chce Litva společně s Estonskem a Lotyšskem vybudovat 1300megawattový reaktor, aby se staly nezávislejšími na dovozu energie z Ruska.

Předpokládá se, že v roce 2020 bude do sítě připojen také první reaktor jaderné elektrárny na severozápadě Polska. Do roku 2035 mají dva reaktory vyrábět dohromady 6000 megawattů elektřiny z jádra. V současnosti jsou prováděny průzkumy lokalit. V obcích, jichž se to týká, narůstá neklid - a nejen tam, protože Gaski, Choczewo a Żarnowiec, v nichž je výstavba elektrárny zvažována, leží v blízkosti německé hranice.

Spolkové země Berlín a Braniborsko už Varšavě sdělily své námitky proti projektu, v příhraničních obcích Braniborska vznikají občanské iniciativy, na druhé straně hranice lidé vyšli na protest proti jaderným plánům do ulic.

Občané obcí se vyslovili proti výstavbě elektrárny v peticích a v místním referendu. Ale jasné ne podobně jako v Litvě pouze ukázalo obraz nálad, aniž by to mělo právní důsledky.

Co se ČR týče, jaderná elektrárna Temelín má být do roku 2025 rozšířena o třetí a čtvrtý reaktorový blok. Elektrárna leží necelých 100 kilometrů od hranic s Německem a Rakouskem, což především v Rakousku vyvolává obavy, protože jaderná elektrárna je od spuštění první řetězové reakce v prosinci 2000 kritizována kvůli četným technickým poruchám.

Také na Slovensku, které je atomové energii tradičně příznivě nakloněno, není předmětem debaty samotné plánované posilování jaderné energetiky, ale proč se zpožďuje. Italský

provozovatel Enel totiž slíbil uvedení třetího a čtvrtého bloku jaderné elektrárny Mochovce do provozu už v letech 2012 až 2013. Místo toho teď může zaručit dokončení nejdříve v roce 2017. Enel to odůvodnil tím, že od katastrofy ve Fukušimě vzrostly bezpečnostní požadavky, které vedly k dodatečným stavebním opatřením. Na plánech dostavby to nic nemění.

EDF má souhlas ke stavbě první britské jaderné elektrárny od roku 1995

Britské ministerstvo energetiky vydalo francouzské společnosti EDF územní povolení pro stavbu nové jaderné elektrárny na jihozápadě země. Projekt v lokalitě Hinkley Point na anglické straně Bristolského zálivu by se měl stát první novou jadernou elektrárnou v zemi od roku 1995. EDF, kterou z většiny vlastní francouzská vláda, ovládla britskou jadernou energetiku v roce 2009, kdy koupila jadernou skupinu British Energy. Společnost požádala vládu o souhlas s projektem v říjnu 2011 a komise pro územní plánování doporučila schválení projektu loni v prosinci.

Kauza ČEZu v Bulharsku

„Byli jsme nuceni k tomuto kroku přistoupit vzhledem k tomu, že opakovaně čelíme negativním zásahům ze strany bulharských institucí. Požádali jsme Evropskou komisi o nezávislé posouzení celé situace s cílem zajistit našim bulharským společnostem objektivní a spravedlivé postupy,“ vysvětluje důvody pro podání stížnosti Tomáš Pleskač, ředitel divize distribuce a zahraničí. Jedná se zejména o způsob zahájení procedury odebrání licence, k níž dal popud premiér a nikoliv nezávislý energetický regulační úřad, který jediný je k prověřování této záležitosti oprávněný. K odebrání licence vyzýval rovněž generální prokurátor. Takové jednání je v rozporu s evropským právem, jehož jednotlivá opatření dosud nebyla implementována do bulharské legislativy, což vytváří podmínky pro narušování nezávislosti této instituce. Bulharská republika se stejně tak jako Česká republika dobrovolně zavázala plnit veškeré zákony, direktivy i principy vyplývající z členství v Evropské unii. Kromě toho se většina údajných pochybení ČEZ, které mají být důvodem pro odebrání licence, týká nákupů v rámci veřejných zakázek, které však nespadají dle bulharského práva mezi důvody pro odebrání licence. Ty musejí být velmi závažné, patří mezi ně ohrožení bezpečnosti dodávek elektřiny, soustavné porušování licenčních podmínek, neplnění pokynů regulátora nebo poskytnutí nesprávné informace při žádosti o licenci.

Zahraniční experty inspirují hodonínské zkušenosti s biomasou

Třicítka expertů Mezinárodní energetické agentury si nenechala ujít speciální exkurzi v provozu zaměřenou na spalování biomasy v Elektrárně Hodonín. Stalo se tak u příležitosti konference Kotle a energetická zařízení 2013. Elektrárna Hodonín vyrobila loni z biomasy přes 216 milionů kWh elektřiny, a pokryla tak roční spotřebu více než 60 tisíc jihomoravských domácností.

Cvičení na JE Temelín

Více než 600 tisíc Jihočechů se náhle ocitá bez elektřiny. Továrny se zastavují, území se ponořilo do tmy. Může za to hned několik zkratů rozvodných linek. Kraj postihl tolik obávaný blackout. Takový byl scénář štábního energetického cvičení, které proběhlo na elektrárně Temelín. Do cvičení se zapojilo 30 specialistů ze společností ČEZ, ČEPS a E.ON. Energetici procvičovali zajištění elektřiny pro elektrárnu Temelín z vodní elektrárny Lipno.

Řada států dle MMF zvyšuje zlaté rezervy, Česko ne

Řada států zvyšuje své zlaté rezervy, Česko však na rozdíl od mnoha jiných zemí své zásoby snížilo. Vyplývá to z nejnovější analýzy Mezinárodního měnového fondu, kterou MMF zpracoval na základě údajů od národních bank. Největší zlaté rezervy mají Spojené státy a Německo.

Česká republika snížila podle analýzy zlaté rezervy o 0,218 tuny. Zásob zlata se dále zbavovala například Kanada, která snížila své rezervy o 0,124 tuny.

Ke konci loňského roku Česká národní banka podle jejího dnešního vyjádření pro ČTK spravovala 11,5 tuny zlata. O rok dříve to bylo 12,4 tuny. Objem zlatých rezerv v držení ČNB

postupně klesá, poněvadž ČNB toto zlato tradičně spotřebovává pro výrobu zlatých mincí pro širokou veřejnost,' uvedl Tomáš Zimmermann z tiskového oddělení ČNB.

Rusko v únoru hlásilo setrvalý nárůst rezerv po dobu čtyř měsíců. Přidalo téměř sedm tun a celkově má 976,952 tun zlata.

Zlato, které zvyšovalo hodnotu 12 let, letos už přišlo o čtyři procenta své bývalé ceny, a to je podle Reuters důkazem oživující světové ekonomiky.

Turecko zvýšilo zásoby zlata o 5,574 tun na celkových 375,731 tun; měsíční nákup zlata je ale oproti předchozím měsícům nižší. V únoru zlato nakupovaly i Kazachstán, Ázerbájdžán, Bělorusko, Kyrgyzstán, Mongolsko a Ukrajina. Například Kazachstán nakoupil 4,914 tun a nyní má celkem 121,670 tun zlata ve svých rezervách. Ale například Indonésie, která zásoby zvýšila o 2,799 tun, má celkem 'jen' 75,894 tun. Nejvíce zlata mají podle MMF ve svých rezervách Spojené státy, a to 8133,5 tun. Po nich následuje Německo s 3391,3 tunami.

Zlato je podle ČNB nevýznamnou a pasivně drženou částí objemu devizových rezerv ČNB, tvoří méně než procento těchto rezerv. Devizové rezervy slouží především k podpoře provádění vlastní měnové a kurzové politiky. Zlato přitom není podle ČNB nejvhodnější nástroj, protože nenese úrok a na druhou stranu jsou s jeho držením spojeny dodatečné náklady například za uskladnění. Samotné operace s devizovými rezervami ČNB ovšem průběžně nezveřejňuje.

S tím částečně souvisel i významnější prodej zlata Českou národní bankou v letech 1997 a 1998. V době těchto prodejů existovaly i obavy, že centrální banky zemí vstupujících do evropské měnové unie mohou po vstupu prodat větší část ze svých zásob zlata. 'V té době na trhu převládala psychologie 'kdo prodá později, bude v horší situaci', notně podporovaná vývojem cen zlata od počátku 90. let. Proto bylo rozhodnuto zaměnit pasivně spravované zlato za likvidní investice přinášející nezanedbatelný výnos,' uvedl Zimmermann. V září 1998 například ČNB prodala 31 tun zlata, za celý rok 1997 to bylo 25 tun.

Výbuch plynu v čínském uhelném dole

Následkem výbuchu plynu v uhelném dole na severovýchodě Číny zahynulo 28 horníků. Čínské doly dlouhodobě patří k nejnebezpečnějším na světě. Vláda uvádí, že díky její kampani za uzavírání malých a nelegálně provozovaných dolů a za modernizaci důlních zařízení ostatních dolů se bezpečnost těžby uhlí v poslední době výrazně zlepšuje. Minulý měsíc oznámila, že v loňském roce se počet obětí důlního průmyslu snížil o více než 30 procent na 1384 lidí.

Německo letos spustí nejvíce uhelných elektráren za dvacet let



Rekordní rok letos zažije německá uhelná energetika. Německo v letošním roce uvede do provozu nejvíce uhelných elektráren za poslední dvě desetiletí.

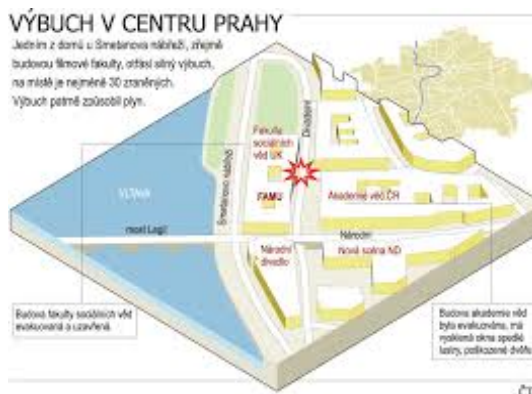
Německé jaderné elektrárny, které byly uzavřeny v roce 2011, ve velkém nahrazuje uhlí. Letos začnou v Německu fungovat nové uhelné elektrárny o výkonu 5 300 megawattů. (Pro srovnání: oba reaktory Temelína mají dohromady výkon 2 000 MW. V celé ČR je cca 11 000 MW uhelných elektráren.) Odstaveny budou starší uhelné elektrárny o celkovém výkonu 1 000 megawattů.

Duben

Výbuch plynu v Divadelní ulici v Praze

Dne 29.4.2013 došlo v Praze k výbuchu plynu po úniku z plynového řádu. Výbuch poničil kolem desáté dopoledne budovu mezi Smetanovým nábřežím a Divadelní ulicí v centru Prahy. Exploze byla slyšet po celém centru, tlaková vlna vysypala okna v okruhu stovek metrů. Stěna domu, kterým otlásl výbuch, byla podle informací statika Petra Macháně posunuta o pět centimetrů. Nosné konstrukce domu poškozeny nebyly.

Počet zraněných dosáhl 43, škody byly vyčísleny na 100 milionů korun. Evakuováno bylo 230 osob.



Společnost Pražská plynárenská po výbuchu realizovala kontrolu plynového potrubí a odhalila přibližně stovku drobných úniků plynu, naprostá většina z nich ale byla u rozvodů v domácnostech. V 88 případech byl drobný únik zjištěn u bytových instalací nebo domovních rozvodů, zejména ze závitových spojů. Ve 14 případech byl lokalizován drobný únik v rámci uličních rozvodů, nejčastěji na místě dělicím distribuční soustavu a odběrné plynové zařízení.

Muslimští radikálové zaútočili na pěšávarskou elektrárnu

Nejméně sedm lidí zahynulo při útoku desítek pákistánských muslimských radikálů na elektrárnu ve městě Pěšávar. Na místě byli zabiti zaměstnanec a policista. Útočníci s sebou odvedli deset rukojmí. Pět z nich bylo nalezeno mrtvých na nedalekém poli, uvedla BBC.

„Napadli elektrárnu kolem 2:30 ráno. Zabili dva lidi na místě a odvedli deset dalších,“ řekl AFP policejní důstojník Džavid Chán. Podle něj byli dobře a těžce vyzbrojeni.

K útoku na elektrárnu se nikdo nepřihlásil, v oblasti poblíž kmenových území ale operuje pákistánský Tálibán, který podnikl už několik útoků ve čtvrti, kde elektrárna stojí. Zesílení aktivit radikálů pravděpodobně souvisí s blížícími se volbami do parlamentu.

Květen

Těžaři chtějí plyn z východu Čech. Jde jim o břidlice, varují odpůrci

Skoro 180 obcí od Hradce Králové a Pardubic až téměř po Svitavy se ocitlo v hledáčku firmy South Oil. Ta si vyhlédla 1 341 kilometrů čtverečních na Hradecku, Pardubicku, Orlickoústecku, Chrudimsku a Svitavsku kvůli konvenčním zásobám plynu a ropy. Podle geologů tam však nic takového není. Aktivisté z Koalice STOP HF však tvrdí, že těžařům může jít o jižní cíp území v okolí Svitav a tím také o nekonvenční břidlicový plyn.

Území Hradecka a Pardubicka, které si těžaři vybrali, je v posledním období v Česku vůbec nejrozsáhlejší. Jiné dvě firmy už řadu měsíců usilují o tři průzkumná území pro břidlicový plyn.

Firma Basgas Energia Czech s australsko-americkými vlastníky před rokem dostala od státu svolení na území Trutnovska, ale ministr životního prostředí je po protestech občanů zrušil a žádost se znovu projednává. Průzkumné území se zúžilo a řízení je přerušeno.

Stejná firma chce zkoumat i Berounsko, další usiluje o území kolem Valašského Meziříčí. Ministr životního prostředí Tomáš Chalupa vyhlásil na všechny aktivity kolem břidlicového plynu dvouleté moratorium, než se podaří upravit zákony i pro novou technologii.

Zahraniční solární investoři zahájili arbitráž proti Česku

Sdružení provozovatelů solárních elektráren International PhotoVoltaic Investors Club (IPVIC) oficiálně oznámilo zahájení arbitráže proti Česku. Osm investorů požaduje odškodné za finanční újmu, kterou jim údajně způsobilo zavedení 26% odvodu z výnosů solárních elektráren.

Výši částky, o níž chtějí investoři vést arbitráž, IPVIC nezveřejnil, stejně jako místo konání arbitráže. 'Kalkulace škody ještě nebyla dokončena,' řekl ČTK mluvčí IPVIC Donath. Podle serveru IHNED.cz půjde v arbitráži zhruba o 2,5 miliardy korun a řízení potrvá nejméně dva roky.

Výbuch nálože poškodil ropovod v Jemenu, zastavil dodávky ropy

Neznámí ozbrojenci v Jemenu zaútočili na hlavní ropovod určený pro přepravu ropy do zahraničí a zastavili tak dodávky ropy. Podle agentury Reuters to dnes oznámilo tamní ministerstvo obrany a nejmenované zdroje z odvětví.

Útočníci podle sdělení ministerstva vyhodili do povětří část ropovodu, který vede na pobřeží Rudého moře. Incident se stal v provincii Maríb v centrální části země.

Jemen, který je domovem jedné z nejnebezpečnějších větví teroristické sítě Al-Káida, z prodeje ropy financuje až 70 procent státních výdajů. Od začátku protivládního povstání v roce 2011 se v zemi odehrálo velké množství pumových útoků na ropovody. Počet sabotážních akcí namířených na ropovody a ropná zařízení v provincii Maríb podle ministerstva v poslední době dramaticky stoupl.

Červen

Země OECD prvně v historii spotřebovaly méně ropy než zbytek světa

Skupina vyspělých průmyslových zemí sdružená v Organizaci pro hospodářskou spolupráci a rozvoj OECD spotřebovala v dubnu poprvé v historii méně ropy než zbytek světa. V červnu to to uvedl Úřad pro energetické informace při americkém ministerstvu energetiky. Členem OECD je také Česká republika.

Poptávka po ropě ve 34 zemích OECD činila v dubnu 44,3 milionu barelů denně. Ostatní svět zvýšil poptávku na 44,5 milionu barelů za den, uvedl Úřad pro energetické informace (EIA) v rámci zprávy o vývoji na ropném trhu.

Za posledních deset let se ropná poptávka zemí mimo OECD zvýšila o téměř 50 procent. Podle EIA může sice být dubnový vývoj zatím jenom sezonní výkyv vyvolaný jarním poklesem poptávky ve vyspělých zemích, v příštím roce by však rozvojový svět měl většinový podíl na ropném trhu potvrdit.

Před deseti lety spotřeboval rozvojový svět pouze dvě třetiny toho, co vyspělé země. Zatímco chudší země svou spotřebu díky silnému ekonomickému růstu výrazně zvyšovaly, státy OECD reagovaly na růst cen, obavy o klima a finanční a ekonomickou krizi omezením poptávky.

EIA čeká v letošním roce růst globální poptávky o 870 000 barelů na 89,2 milionu barelů denně. Před deseti lety byla světová poptávka na úrovni zhruba 78 milionů barelů denně.

EIA předpověděl, že růst těžby ropy v zemích mimo ropný kartel OPEC bude letos vyšší než globální nárůst poptávky a zvýší se o 1,2 milionu barelů na 53,91 milionu barelů denně. Nárůst produkce povede Severní Amerika díky expanzi těžby z břidlic v USA a ropných písků v Kanadě.

OPEC předpověděla, že světová poptávka po ropě se bude ve druhé polovině letošního roku zvyšovat mnohem rychleji než v prvním pololetí. Za celý letošní rok OPEC čeká zvýšení poptávky o 780 000 barelů denně. Objem těžby za celý kartel OPEC se v květnu zvýšil o 106 000 barelů na 30,57 milionu barelů denně.

Ministerstvo kývlo na průzkum území pro jaderné úložiště na Kraví hoře

Ministerstvo životního prostředí vyhovělo žádosti o stanovení průzkumného území pro úložiště jaderného odpadu v lokalitě Kraví hora na Žďársku. Na první ze sedmi vytipovaných lokalit tak může začít první etapa průzkumných prací.

Žádost o stanovení průzkumného území počítá pouze s provedením první etapy průzkumných prací. Ta zahrnuje povrchové a přípovrchové měření, sondáže a odběr hornin pomocí neinvazivních metod a bez zásahu do pozemků.

"Jelikož tato etapa bude společná pro všechny lokality, umožní výsledky průzkumů lokality vzájemně srovnat a zúžit počet dotčených obcí či méně vhodné vyřadit," říká mluvčí Správy úložišť radioaktivních odpadů (SÚRAO) Tereza Bečvařiková.

Po nabytí právní moci tohoto rozhodnutí se obcím z lokality otevírá i možnost získat finanční příspěvky vyplývající ze zákona, které mohou použít na svůj rozvoj. Celková suma pro všech osm obcí z Kraví hory je bezmála deset milionů korun ročně. Tato suma bude obcím vyplácena po celou dobu trvání průzkumných prací.

Albánská CEZ Shpërndarje čelí arbitráži o 2,8 miliardy korun

Albánská společnost Debt International Advisory (DIA), která se živí vymáháním dluhů, spustila arbitráž proti společnosti CEZ Shpërndarje. Ve sporu požaduje zaplacení 108,5 milionů eur, tedy 2,8 miliardy korun, mimo jiné kvůli jednostrannému vypovězení smlouvy mezi oběma firmami.

V CEZ Shpërndarje vlastní česká společnost ČEZ 76 procent akcií, v lednu ale po jmenování státního administrátora ztratila nad albánskou firmou kontrolu.

Podle arbitrážního návrhu uzavřela CEZ Shpërndarje v roce 2010 smlouvu s DIA o vymáhání dluhů od těch zákazníků, kteří po více než 90 dní neplnili své závazky vůči distributorovi. V únoru 2011 společnosti prodloužily platnost smlouvy o další dva roky, na konci října 2011 ale po neshodách CEZ Shpërndarje kontrakt jednostranně vypověděla.

DIA se nyní domáhá vyplacení odměn za úspěšně vypořádané dluhy a odškodného za předčasné ukončení kontraktu. Celkem DIA požaduje vyplacení 108,5 milionu eur. Bude o ně usilovat při arbitráži, která se povede ve Vídni.

Letos v květnu začal arbitrážní spor také z popudu ČEZ, který chce získat odškodnění za zmařenou investici v Albánii. Firma se odvolává na Smlouvu o energetické chartě, žalovanou sumu neuvedla.



ČEZ v Albánii

V roce 2009 získal 76 procent tamní distribuční společnosti, minorita patří státu. ČEZ se ale v Albánii potýkal se špatnou platební morálkou odběratelů. Do dalších problémů se dostal na počátku loňského roku, kdy albánský regulační úřad zhruba dvojnásobně zvýšil tarify, které distributor

platil státním elektrárenským společností, zakázal ale CEZ Shpërndarje promítnout toto zdražení do koncových cen.

CEZ Shpërndarje po sérii sporů s albánským státem letos v lednu přišla o licenci k distribuci elektřiny a začal ji kontrolovat státní administrátor.

Evropská komise představí návrhy pro posílení jaderné bezpečnosti

Evropská komise představila návrhy pro posílení jaderné bezpečnosti na starém kontinentu. Vychází přitom z výsledků zátěžových testů, které se uskutečnily v evropských jaderných zařízeních. Testy byly reakcí na předložskou havárii jaderné elektrárny v japonské Fukušimě.

Očekává se, že komise navrhne dodatky ke stávajícím pravidlům pro jadernou bezpečnost. Komise podle týdeníku European Voice chce kromě jiného zajistit v této oblasti nezávislost státních úřadů a určit bezpečnostní opatření pro jednotlivá období provozu jaderného zařízení.

Jaderný průmysl se obává, že některá technická opatření jsou v návrhu pojata příliš podrobně. Provozovatelé jaderných zařízení se domnívají, že by konkrétní opatření měly určovat jednotlivé členské země EU. V unijní směrnici by podle nich měly být jen hlavní bezpečnostní cíle.

Evropská komise navrhla pravidelné kontroly jaderných elektráren

Evropská komise navrhla nová opatření pro jadernou bezpečnost, která zahrnují povinnost každých šest let v Evropské unii kontrolovat jaderné elektrárny. Opatření jsou podle agentury Reuters reakcí na předložskou havárii v japonské elektrárně Fukušima. EU po havárii uskutečnila sérii zátěžových testů, aby prověřila odolnost evropských jaderných elektráren. Dnešní návrhy jsou založeny na výsledcích těchto testů.

"V Evropě je dnes v provozu 132 jaderných reaktorů. Úkolem komise je zajistit, aby u každého

z nich byla nejvyšší prioritou bezpečnost,' uvedl evropský komisař pro energetiku Günther Oettinger.

Zátěžové testy zkoumaly, jak jsou elektrárny připraveny vypořádat se s extrémními případy, jako jsou ničivá zemětřesení či záplavy. Testy ukázaly, že žádnou z evropských elektráren není třeba uzavřít a že úroveň bezpečnosti je obecně vysoká. Odhalily však řadu nedostatků, jejichž odstranění si vyžádá částku od deseti do 25 miliard eur (od 257 do 643 miliard Kč).

Nové jaderné elektrárny budou muset být podle návrhu komise koncipovány tak, aby případné poškození reaktoru nemělo žádné dopady na okolí. Regulační orgány jednotlivých členských států EU budou mít rovněž za úkol navrhnout strategii pro komunikaci s veřejností v případě nehody. Občanům má být navíc poskytnut prostor v rozhodovacím procesu při udělování povolení pro nové jaderné elektrárny.

Před zavedením budou muset nová pravidla schválit všechny členské země. Pravidla zahrnují i to, že EU bude moci poslat do určité země inspektory, pokud se jí bude zdát, že kontrola byla nedostatečná nebo s ní země otálí. Mnoho poslanců Evropského parlamentu a ekonomů nová pravidla kritizuje a považuje je za nedostatečná.

Plynovod Nabucco plyn z Ázerbájdžánu do Evropy přepravovat nebude

Projekt plynovodu Nabucco West nebude dodávat zemní plyn z Ázerbájdžánu do Evropy. Oznámila to rakouská ropná společnost OMV, která konsorcium Nabucco West vede. Nabucco soutěžil o plyn z Kaspického moře s konkurenčním projektem jiných evropských energetických společností Trans-Adriatic Pipeline (TAP).

Konsorcium pro těžbu plynu na ázerbájdžánském poli Šach Deniz projekt Nabucco pro přepravu plynu do Evropy nevybralo, uvedla OMV. Zda ale získala přednost TAP, firma nesdělila.

Skupina pro těžbu v Ázerbájdžánu tvořená britskou BP, norskou společností Statoil, ázerbájdžánským státním podnikem SOCAR a francouzským Totalem se měla do konce června rozhodnout, kterému z projektu dá přednost. Skupina chce vyvážet od počátku roku 2019 z velkého ázerbájdžánského pole Šach Deniz 16 miliard krychlových metrů plynu ročně plynovodem Transanatolian Pipeline (TANAP) na hranice Turecka a Bulharska, kde se má napojit plynovod dál na západ.

Řecká vláda se nyní dohaduje na prodeji dvoutřetinového podílu v řeckém provozovateli plynovodů DESFA ázerbájdžánské firmě SOCAR. Ta chce dodávat plyn do Řecka přes Turecko a Atény si od této dohody slibovaly, že právě prodejem do jejich rukou bude mít projekt TAP větší šance než návrh konkurence.

Požáry trafostanic v Praze

Ve druhé polovině června byly zaznamenány v Praze dva požáry trafostanic. První z nich se odehrál v pražské části Šeberov (Praha 4), přičemž došlo ke zničení trafostanice a škoda dosáhla 100 milionů korun. Druhý, podstatně menší požár, se udál na sídlišti Lehovec. Bez elektřiny tak zůstaly části sídliště Lehovec, Černý most, část Satalic a Hloubětína. Jako souhrnu náhod označuje požár obou trafostanic Zuzana Dvořáková, ředitelka komunikace ČEPS. Podle odhadů společnosti byl první požár pravděpodobně způsobený technickou závadou, vadná součástka se nicméně mohla rozbít i vlivem tepla. Příčiny požáru se ale technici společnosti nedozví, dokud celý transformátor důkladně neprozkoumají, dodala Dvořáková.

Hasiči z Havířova zasahovali u požáru trafostanice u areálu bývalého dolu Dukla

Plameny byly zpozorovány v Šachetní ulici, zda došlo k požáru vlivem současných vysokých teplot, nebylo potvrzeno. Oficiálně byla příčinou technická závada. „Podle výsledků vyšetřování může za požár technická závada. Na místě zasahovaly dvě jednotky Hasičského záchranného sboru Moravskoslezského kraje, konkrétně z Havířova a Karviné. Požár hasiči zdolali za zhruba dvacet minut,“ informoval mluvčí krajských hasičů Petr Kúdela.

Zdroj: idnes.cz, MV-GR HZS ČR, ihned.cz, lidovky.cz, ČTK, novinky.cz

Přehled rozsáhlých výpadků dodávek elektrické energie v ČR

- ✓ 4. prosince 2002 - Požár rozvodny v ulici U Rajske zahrady v Praze ochromil odpoledne život zejména v centru hlavního města. Nejezdily tramvaje, nesvítilo světlo, netekla voda, nefungovaly semaforey a v některých domácnostech také přestalo fungovat topení. Pravděpodobnou příčinou požáru byla porucha izolace na jednom z kabelů. Nejdéle, zhruba půl dne, byly bez proudu Vinohrady. Domácnosti na pražském Žižkově a Vinohradech byly druhý den zhruba hodinu opět bez elektrického proudu, a to kvůli poruše náhradního zdroje.
- ✓ 13. srpna 2003 - Centrum hlavního města a přilehlé oblasti, celkem asi čtvrtina Prahy, se odpoledne ocitlo bez elektrické energie. Důvodem byl výpadek jednoho z transformátorů.
- ✓ 25. července 2006 - Podle odborníků byla ČR na pokraji blackoutu. Elektrickou rozvodnou síť ochromil mimořádný výpadek. ČEPS brzy odpoledne vyhlásil stav nouze a odvolal jej ve 23:00, kdy se situace přenosové soustavy výrazně zlepšila. Výpadek nastal kvůli přetížení sítě a kumulaci menších výpadků některých přenosových vedení; ke krizi přispěla i vedra. Žádnému spotřebiteli nebyla dodávka elektřiny přerušena, velcí spotřebitelé museli omezit odběr.
- ✓ 18. a 19. ledna 2007 - Orkán Kyrill, který pustošil takřka celou Evropu, způsobil i kritickou situaci na energetických sítích. Jenom společnost ČEZ měla v jednu chvíli bez proudu až milion zákazníků.
- ✓ 1. března 2008 - Celou Evropu včetně Česka zasáhla vichřice Emma. Výpadky elektrické sítě postihly na vrcholu kalamity téměř milion lidí; energetická společnost ČEZ vyhlásila stav nouze v krajích Královéhradeckém, Pardubickém, Plzeňském a Karlovarském a v okrese Semily.
- ✓ 16. října 2009 - Řadu okresů v několika krajích postihly výpadky proudu způsobené počasím. Bez proudu bylo zhruba 60.000 domácností. Nejhorší situace byla na Vysočině, kde hustě sněžilo.
- ✓ 18. června 2013 - U Kunratického lesa v Praze kolem 22:30 vybuchla trafostanice a vypukl požár. Velkou část Prahy postihl výpadek proudu. Dodávky se podařilo obnovit krátce po půlnoci. Bez proudu se ocitla zhruba třetina obyvatel Prahy.

Ve výčtu nejsou zahrnuty výpadky dodávek elektrické energie v době povodní.

Zdroj: ČTK

Výběr případů výbuchů plynu s obětmi za posledních deset let

- ✓ 11. června 2003 - Dva manželé a jejich dvouleté dítě se udusili při požáru rodinného domku v Praze 4-Spořilově. Oheň se rozšířil po výbuchu plynu, který unikal z karmy.
- ✓ 21. června 2004 - Výbuch plynu v činžovním domě v brněnské Tržní ulici si vyžádal čtyři oběti. Přímo v troskách zemřela šestašedesátiletá žena a čtyřletá holčička, v nemocnici další žena a muž.
- ✓ 28. října 2004 - V bytě na sídlišti Jižní Svahy ve Zlíně vybuchla propanbutanová láhev. Zemřel třiatřicetiletý muž.
- ✓ 22. srpna 2005 - V obci Zlosyň u Veltrus ve sklepě rodinného domu vybuchla desetikilogramová plynová bomba. Výbuch zasypal dva muže, jeden z nich zemřel.
- ✓ 17. října 2005 - Při výbuchu plynu a požáru domku v Libodřicích na Kolínsku zemřel roční chlapec. Popálena byla matka a další dítě.
- ✓ 18. února 2006 - Při výbuchu plynu v restauraci U Arbese v přízemí obytného domu v Praze 5 zemřeli dva muži, čtyři lidé utrpěli zranění.
- ✓ 20. dubna 2006 - Explozi plynu a požár v rodinném domě v Paskově na Frýdecko-Místecku nepřežila pětadvacetiletá majitelka vily.
- ✓ 25. srpna 2006 - V bytě v Pelhřimovské ulici v Praze 4 po výbuchu plynu a následném požáru zemřeli dva lidé.
- ✓ 23. května 2008 - Při explozi metanu přišel o život pracovník čističky odpadních vod v Roztokách u Prahy.
- ✓ 16. listopadu 2008 - Jednoho mrtvého a šest zraněných si vyžádal výbuch plynu v Hradci Králové ve Střelecké ulici.
- ✓ 27. října 2009 - Výbuch propanbutanové láhve v kuchyni restaurace Za mostem v Brně-Štýřicích si vyžádal život čtyřiapadesátileté ženy.
- ✓ 27. ledna 2010 - V domku v Uherském Brodě na Slovácku vybuchl plyn. Uvnitř objektu byl nalezen mrtvý čtyřiatřicetiletý muž.
- ✓ 22. září 2011 - Při výbuchu v ulici U Šamotky na hranici Liberce a Jablonce nad Nisou přišla o život dvaadvacetiletá žena. Policie vyloučila spekulace o tom, že v domě explodovala varna pervitinu a přiklonila se k tomu, že šlo o výbuch plynu.
- ✓ 17. února 2013 - Výbuch plynu v panelovém domě ve Frenštátě pod

Zdroj: ČTK

Exkurz

Cvičení Zóna 2013

V rámci prověření aktivní ochrany proti havárii na atomovém objektu a praktické synchronizaci složek krizového řízení při této situaci, proběhlo ve dnech 26. - 28. března v areálu jaderné elektrárny Dukovany cvičení s názvem Zóna 2013. Jednalo se o cvičení simulující „black-out“, který vedl k mechanickému selhání u jednoho z reaktorů a úniku radioaktivní látky do životního prostředí. Cvičení mělo za cíl nacvičit koordinaci záchranných a likvidačních prací po vzniku mimořádné události, činnost orgánů krizového řízení při přijímání neodkladných krizových opatření a následných opatření, ověřit schopnost spolupráce a minimalizace škod, prostřednictvím kooperativního přístupu jednotek krizového řízení, policie ČR, IZS, AČR a správních složek kraje, včetně zainteresovaných ministerstev.

Cvičení, jehož hlavním garantem bylo Ministerstvo vnitra – Generální ředitelství hasičského záchranného sboru ČR, bylo největší akcí svého druhu v posledních 5 letech, zúčastnilo se ho 1590 osob a 97 kusů techniky, trvale vyčleněných pro pomoc jednotkám PČR a IZS. Kromě policistů z Krajských ředitelství policie kraje Vysočina a Jihomoravského kraje se do cvičení Zóna 2013 zapojil také krizový štáb policejního prezidenta, operační odbor Policejního prezidia ČR a mobilní radiační skupina Policie ČR začleněná do celostátní radiační monitorovací sítě.

V rámci Krajského ředitelství policie kraje Vysočina se na cvičení podílelo dle rozkazu ředitele a v souladu s plánem cvičení 41 policistů, 11 služebních vozidel a 13 vojáků Armády ČR z Univerzity obrany Brno povolanych k plnění úkolů policie. V rámci Krajského ředitelství policie Jihomoravského kraje se na cvičení podílelo v souladu s plánem cvičení celkem 120 policistů. Celkem se v Policii ČR štábně či fyzicky zapojilo více než 200 policistů.

Scénář cvičení vycházel ze cvičného postihu elektrárny nepříznivými klimatickými podmínkami, které vedly k sérii závad na druhém výrobním bloku elektrárny. Došlo k cvičné ztrátě elektrického napájení bloku a cvičné postupné ztrátě všech tří havarijních dieselových generátorů, což evokovalo v tzv. black-out, tedy ztrátu zdrojů střídavého elektrického napětí. Nepříznivé klimatické podmínky poté způsobily simulovanou destrukci střechy strojovny 2. bloku, což vedlo k poškození parního potrubí a následnému úniku páry. Díky prasknutí trubek jednoho z parogenerátorů, které sloužily k oddělení radioaktivního a čistého oběhu vody, došlo ke smíšení těchto oběhů, průniku radioaktivity na střechu strojovny a do okolí elektrárny.

Vzhledem ke cvičnému nezvládnutí situace krizovým štábem elektrárny a únikem látky do okolí byla vláda nucena vyhlásit nouzový stav, což dále vedlo k zapojení složek IZS a armády.

Přímo na místě zasahovala podniková hasičská jednotka a hasičská jednotka z blízké Třebíče, zatímco došlo k evakuaci zaměstnanců do krytů a následné evakuaci ohrožených osob v areálu.

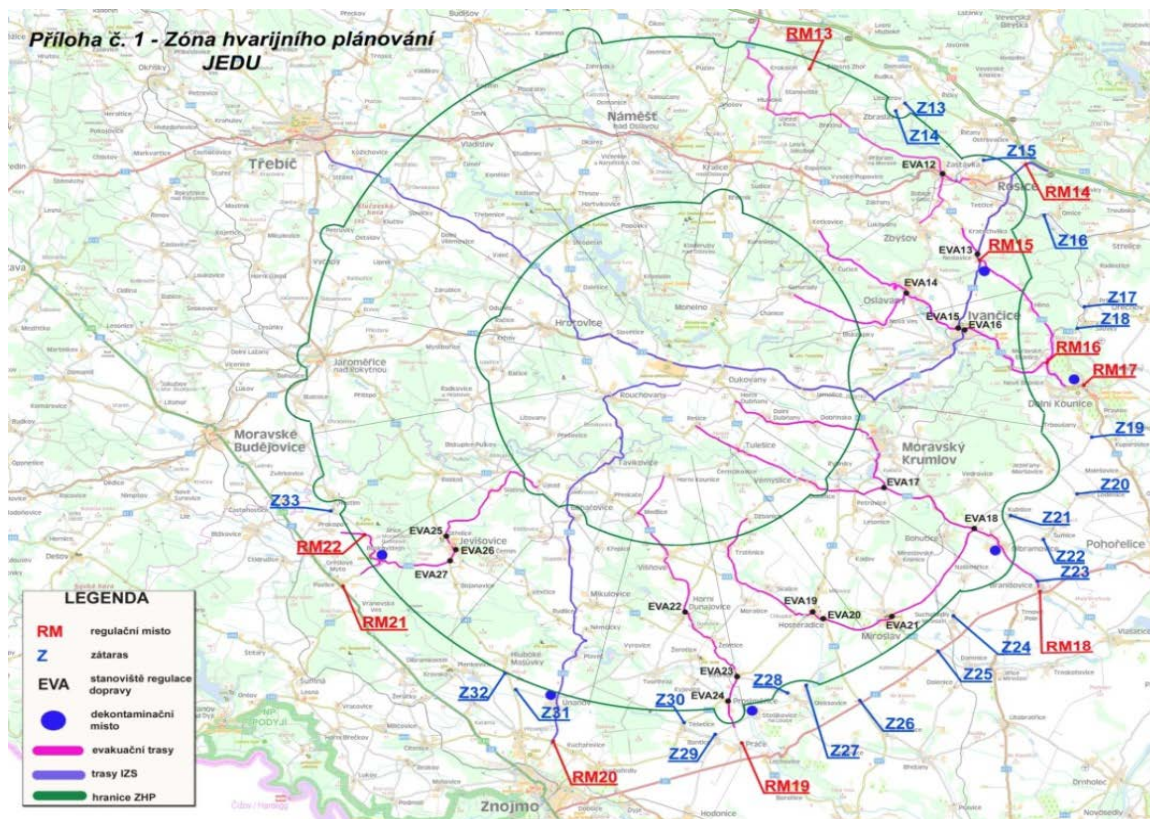
Po konzultaci mezi krizovými štáby Jihomoravského kraje a kraje Vysočina došlo k vyhlášení stavu nebezpečí, zároveň byla odeslána žádost premiéru ČR o vyhlášení nouzového stavu na celém území republiky. Simultánně zasedl také ústřední krizový štáb, pod vedením ministra vnitra.

Na místě havárie mezitím došlo k evakuaci ohroženého obyvatelstva a jejich následné dekontaminaci. Součástí cvičení byla také cvičná dopravní nehoda a následná dekontaminace jejich účastníků. Do akce se zapojily také střediska evakuovaných osob. Vyjma jednotek na místě se do akce zapojilo dále 8 ministerstev, Úřad vlády, na tři desítky dalších úřadů a samosprávné úřady, na jejichž území byl vyhlášen stav nebezpečí, Jihomoravský kraj a kraj Vysočina.

Policie ČR se dále soustředila na tvorbu bezpečného perimetru kolem postižené oblasti a regulaci pohybu osob a vozidel v okolí elektrárny. Ochranná opatření byla realizována ve dvou pásmech o poloměru 5km a 20km.

Mezi jeden z hlavních cílů cvičení patřilo také vyzkoušení komunikace mezi ústředním krizovým štábem a krizovými štáby krajských úrovní, jelikož se jednalo především o cvičení na štábní úrovni. Cvičení se dále poprvé účastnili zaměstnanci státního úřadu pro jadernou bezpečnost s cílem zajistit co možná nejpřesnější predikce vývoje situace a to ve spolupráci

s meteorology. Hejtman Jihomoravského kraje Michal Hašek (ČSSD) zhodnotil cvičení jako velmi úspěšné, když bylo bezproblémově dosaženo splnění všech vytyčených cílů.



Uzávěra byla v Jihomoravském kraji provedena fyzicky. Dále se do cvičení fyzicky zapojila radiální monitorovací skupina Policie ČR.



Zdroj: PČR, AČR, Zpravodaj jaderné elektrárny Dukovany, ceskatelevize.cz, kr-vysocina.cz

BEZPEČNOST FINANČNÍCH INSTITUCÍ

Policejní statistiky a jejich interpretace

Trestné činy za období 1. 1. – 30. 6. 2013 dle „druhu napadených objektů“

druh objektu	zjištěno tr. činů	škody
pojišťovny	397	217 699 500 Kč
banky	711	Souhrnná škoda 929 391 000 Kč
pošty	7	
ostatní finanční instituce	1455	
celkový součet⁴	2570	1 147 090 500 Kč

První prezentovanou statistikou jsou data podle druhu napadených objektů. Z nich lze vyčíst, že v prvním pololetí letošního roku bylo v souvislosti s finančními institucemi evidováno celkem 2570 trestných činů a napáchané škody přesáhly 1 miliardu a 147 milionů korun. Ačkoli počet zjištěných trestných činů a především výše škod mohou působit alarmujícím dojmem, je nutné se na statistiky podívat podrobněji a správně je interpretovat.

Zaměříme-li se na interpretaci dat podle „napadených objektů“, jedná se v případě pojišťoven o 57 případů trestného činu krádeže (§ 205 z. č. 40/2009 Sb., škoda 2 001 800 Kč), 75 případů trestného činu podvodu (§ 209 z. č. 40/2009 Sb., 18 815 700 Kč), 13 případů trestného činu poškození cizí věci (§ 228 z. č. 40/2009 Sb., škoda 242 900 Kč), 176 případů trestného činu pojistného podvodu (§ 210 z. č. 40/2009 Sb., škoda 24 795 500 Kč), 1 případ trestného činu úvěrového podvodu (§ 211 z. č. 40/2009 Sb., škoda 70 000 Kč), 4 případy trestného činu zpronevěry (§ 206 z. č. 40/2009 Sb., škoda 5 371 400 Kč), 2 případy trestného činu porušení povinnosti při správě cizího majetku (§ 220 z. č. 40/2009 Sb., škoda 150 975 100 Kč), 64 případů trestného činu neodvedení daně, pojistného na sociálním zabezpečení (§ 241 z. č. 40/2009 Sb., škoda 13 610 000 Kč). Ve výše uvedeném výčtu jsou zmíněny jen některé trestné činy, jak již vyplývá z tabulky, celkem bylo u pojišťoven evidováno 397 trestných činů, při nichž celková škoda přesáhla 217 milionů korun.

V případě bank došlo ke 22 případům trestného činu loupežného přepadení (§ 173 z. č. 40/2009 Sb.), 133 případům trestného činu podvodu (§ 209 z. č. 40/2009 Sb.), 1 případu trestného činu pojistného podvodu (§ 210 z. č. 40/2009 Sb.) a 555 případům trestného činu úvěrového podvodu (§ 211 z. č. 40/2009 Sb., nejvíce případů se odehrálo v Praze – 178, dále pak v Jihočeském kraji – 79 a Moravskoslezském kraji - 48).

Za první pololetí roku 2013 došlo na poštách k 8 případům trestného činu loupežného přepadení (§ 173 z. č. 40/2009 Sb., 2 případy v Jihočeském kraji, 1 případ v Jihomoravském kraji, 2 případy v Moravskoslezském kraji, 1 v Plzeňském kraji a 2 ve Středočeském kraji) a 7 případům trestného činu podvodu (§ 209 z. č. 40/2009 Sb.). Dále došlo ke 4 případům trestného činu

⁴ Zdrojem veškerých dat v této podkapitole je Policie České republiky.

loupežného přepadení (§ 173 z. č. 40/2009 Sb.) ve směnárnách (v hl. m. Praze, Jihočeském kraji, Jihomoravském kraji a Zlínském kraji).

Co se ostatních finančních institucí týče, došlo v prvním pololetí roku 2013 ke 4 případům trestného činu loupežného přepadení (§ 173 z. č. 40/2009 Sb.), 515 případům trestného činu podvodu (§ 209 z. č. 40/2009 Sb.), 934 případům trestného činu úvěrového podvodu (§ 211 z. č. 40/2009 Sb.) a 2 případům trestného činu dotačního podvodu (§ 212 z. č. 40/2009 Sb.).

Evidována byla v prvních šesti měsících letošního roku také trestná činnost páchaná na bankomatech – konkrétně se jedná o 4 případy trestného činu krádeže (§ 205 z. č. 40/2009 Sb.) a 12 případů trestného činu poškození cizí věci (§ 228 z. č. 40/2009 Sb.), přičemž celková škoda dosáhla 1 326 600 Kč a pachatel byl zjištěn u 3 případů.

Zaměříme-li se na typy jednotlivých trestných činů, bylo např. spácháno v prvním pololetí letošního roku celkem 1579 případů trestného činu podvodu (§ 209 z. č. 40/2009 Sb.), 179 případů trestného činu pojistného podvodu (§ 210 z. č. 40/2009 Sb.), 1535 případů trestného činu úvěrového podvodu (§ 211 z. č. 40/2009 Sb.) a 38 případů trestného činu loupežného přepadení (§ 173 z. č. 40/2009 Sb.).

Navýšení výše uvedených čísel pramení především ze zahrnutí trestných činů páchaných přes internet a sociální sítě. V tomto specifickém prostoru pro páchání finanční kriminality evidovala Policie České republiky celkem 849 případů trestného činu podvodu (§ 209 z. č. 40/2009 Sb.), 2 případy trestného činu pojistného podvodu (§ 210 z. č. 40/2009 Sb.) a 45 případů trestného činu úvěrového podvodu (§ 211 z. č. 40/2009 Sb.).

Loupežná přepadení finančních institucí

Oproti srovnatelnému období loňského roku (1. pololetí 2012) došlo k poklesu počtu spáchaných loupežných přepadení finančních institucí. Důvodem jsou především opatření bank, které ve větší míře zavádějí nové bezpečnostní prvky a technické prostředky, např. kamerové systémy. Výstupy z těchto systému výrazně napomáhají práci policie při objasňování této závažné násilné trestné činnosti. V rámci zlepšování objasněnosti tohoto druhu trestné činnosti je i nadále prohlubována spolupráce 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. Vzhledem ke skutečnosti, že životní úroveň velké části obyvatel České republiky se neustále zhoršuje, je pravděpodobné, že někteří z nich se budou svoji životní úroveň snažit zlepšit i za cenu páchání závažné násilné trestné činnosti.

V první polovině letošního roku byla pracovníky odboru obecné kriminality služby kriminální policie a vyšetřování Krajského ředitelství policie Moravskoslezského kraje zadržena skupina osob, která je důvodně podezřelá ze spáchání série loupežných přepadení finančních ústavů, heren a benzinových čerpacích stanic. Všichni zadrženi byli obviněni a jsou stíháni vazebně. Dosud stále pokračuje šetření k dalším možným spáchaným skutkům.

Pojistné a úvěrové podvody

V prvním pololetí roku 2013 mají zejména pojistné a úvěrové podvody z pohledu kvantitativních ukazatelů struktury hospodářské kriminality stále dominantní postavení. Zároveň nejsou vykazovány významné rozdíly s předchozími hodnocenými obdobími, ať již z hlediska počtu skutků, vyčíslených škod nebo objasněnosti.

Na základě těchto skutečností lze z hlediska dalšího vývoje této formy trestné činnosti predikovat nadále její konsolidovanou úroveň a postavení ve struktuře hospodářské kriminality.

Pokud se týká forem páchání této trestné činnosti, tak ve sledovaném období byla zaregistrována určitá progresa jednání některých fyzických osob z řad zprostředkovatelů pojištění. Jedná se o uzavírání a registraci fiktivních smluv týkajících se tzv. II. důchodového pilíře, tedy smluv

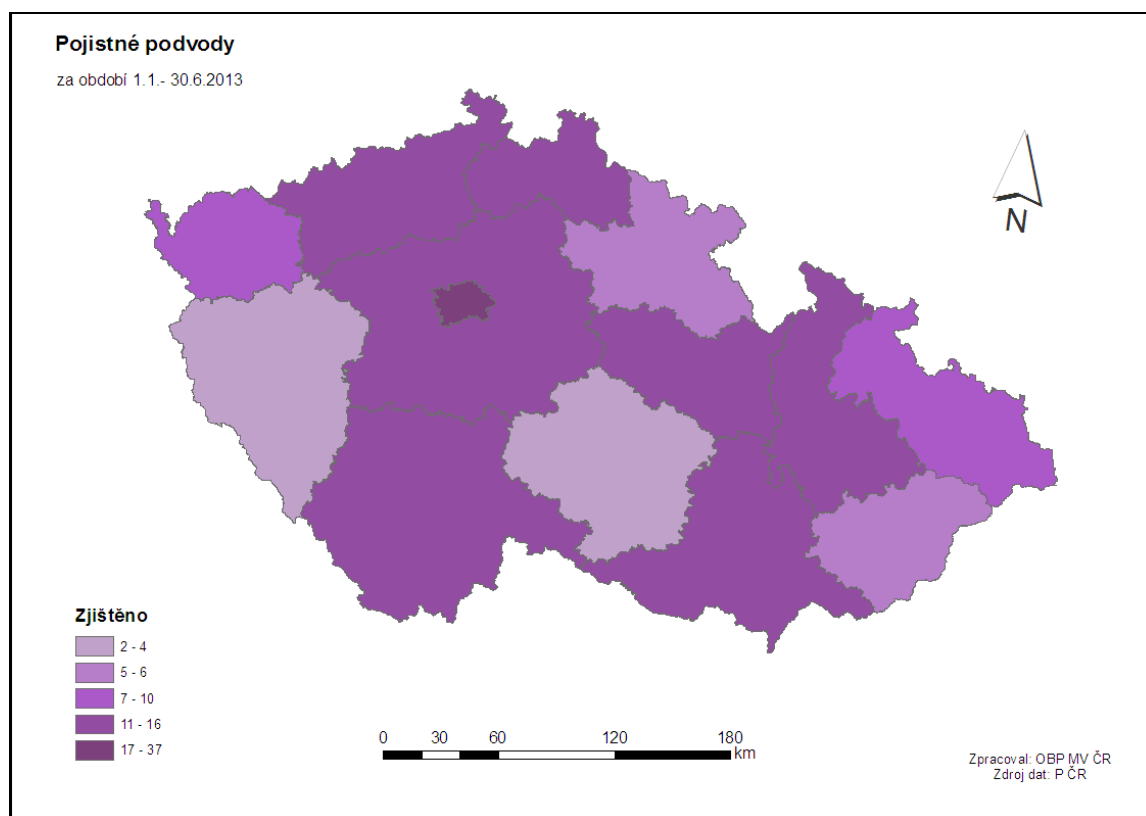
o důchodovém spoření a doplňkového penzijního pojištění se státním příspěvkem, když cílem tohoto jednání je získání finanční odměny - provize z uzavřené smlouvy.

Mezi nejčtenější pojistné podvody stále patří jednání v souvislosti s pojištěním motorových vozidel, vzestupnou tendenci vykazují i podvody v souvislosti s pojištěním osob spojeným s výplatou denního odškodnění v rámci likvidace pracovní neschopnosti pojištěnce. I pro stále sofistikovanější způsoby páčání tohoto druhu kriminality se nadále trestný čin pojišťovacího podvodu však zároveň řadí mezi trestné činy s nejvyšší mírou latence kriminality.

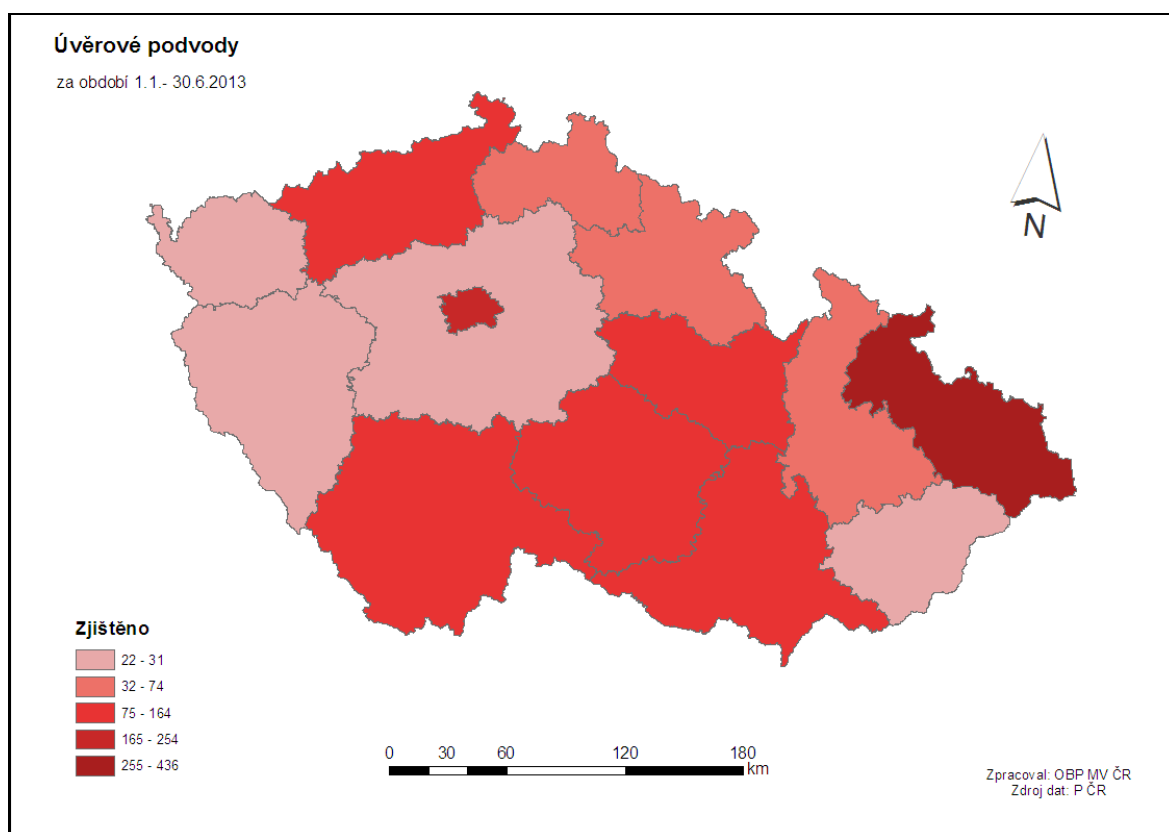
Ke kriminalitě v oblasti úvěrových podvodů dochází převážně u finančních institucí z nebankovního sektoru. Jsou charakterizovány nižšími škodami, což je způsobeno větší obezřetností bankovních a nebankovních ústavů i nižší bonitou klientů jak z řad fyzických, tak i právnických osob, kteří díky tomuto postavení nedosáhnou na vyšší částky úvěrů. I z tohoto hlediska je pak úspěšnost objasňování úvěrových podvodů mnohem vyšší než u úvěrů pojistných, resp. podvodů prostých.

typ trestné činnosti	zjištěno	počet skutků, u nichž byl zjištěn pachatel	celková výše škod
pojistné podvody	179	92	24 795 500 Kč
úvěrové podvody	1535	1073	714 645 000 Kč ⁵

Pro úplnost jsou připojeny dvě mapy, na kterých je znázorněna incidence výskytu tohoto typu trestných činů v rámci České republiky.



⁵ Do výše škod nebyly v důsledku absence dat započítány škody trestných činů úvěrového a pojistného podvodu, jež byly spáchány prostřednictvím internetu a sociálních sítí



Další hospodářská trestná činnost na finančních institucích

V této oblasti nelze opomenout útoky na finanční instituce, tentokrát zejména z bankovního sektoru, a to v souvislosti s jednáním naplňujícím skutkovou podstatu trestného činu neoprávněné držení platební karty. Podíl této trestné činnosti na celkové hospodářské kriminalitě se dlouhodobě pohybuje nad 20% hranicí. A i podle výsledků za první pololetí roku 2013 lze očekávat, že tento trend bude nejen nadále pokračovat, ale lze očekávat i její určitý progres. V daném případě ani značné investice do nových ochranných prvků platebních prostředků, a jejich aplikace v praxi, nedokážou v současné době dostatečně eliminovat jejich neustále se zvětšující využívání.

V oblasti trestné činnosti není v současné době vedena konkrétní statistika případů, kdy se cílem útoku pachatelů stala některá sázková kancelář. V rámci této problematiky byly v prvním pololetí z hlediska hospodářské trestné činnosti řešeny zejména případy neoprávněného provozování loterie a sázkových her, které je páčáno stále sofistikovanějšími způsoby.

Ve sledovaném období se podařilo zrealizovat jeden významný případ v rámci Krajského ředitelství policie hlavního města Prahy, při kterém bylo pachatelům této trestné činnosti zajištěno na celém území České republiky více než 200 kusů výherních přístrojů.

Klesá počet loupežných přepadení bank

V posledních letech dochází k pozvolnému poklesu fyzického přepadávání bankovních domů. Od roku 2007, kdy bylo zaznamenáno 115 bankovních loupeží, došlo k velmi výraznému poklesu, jelikož v roce 2012 bylo evidováno „pouze“ 76 loupeží.

Tento klesající trend vychází především z inovativních opatření na úseku cash managementu, kde se bankám podařilo průřezově snížit průměrnou ztrátu při loupežných

přepadeních. Fakticky tak dochází k situacím, kdy loupeže končí pro banku pouze s minimálními finančními ztrátami, či přímo beze ztrát.

Loupeže ve finančních institucích, především v pobočkách menších nežli banky, například na méně hlídaných poštách se ročně pohybují mezi 120-150, oproti roku 2011 došlo v roce 2012 k mírnému nárůstu, ze 120 na 133 přepadení, nicméně objem odcizené sumy se vlivem zavedení nových metod ochrany financí snížil z 30 milionů na 11 milionů.

Úzká spolupráce mezi Policií ČR a bankovním sektorem, založená především na pravidelné vzájemné výměně informací vede k udržení nízkého počtu loupežných přepadení a zároveň vysokému procentu objasněnosti případů⁶. „Banky spolupracují s Policií ČR především v oblasti prevence a vyšetřování trestné činnosti ve všech jejích podobách.“ Policie pomáhá bankám především s efektivním nastavením preventivních opatření, která se zaměřují především na bezpečnost po fyzické stránce. Jedná se především o kamerové zabezpečení, technologie ochrany hotovosti, sdílenou ochranu a ochranu přístupu do poboček. Mimo opatření technického rázu se Policie ČR dále zaměřuje na přípravu zaměstnanců bank na zvládání krizových situací, spojených s trestnou činností.

Dalším důvodem, proč klesá bankovní kriminalita a její celková úspěšnost je dle mluvčí policejního prezidia tzv. „břídilství“ lupičů. „Skutečnost, že loupežná přepadení tohoto charakteru jsou náročná na přípravu skupin pachatelů. V případě jednotlivců se velmi často jedná o amatérsky provedená loupežná přepadení.“

Zatímco počet klasických bankovních loupeží klesá, včetně škod jimi způsobených, kybernetické útoky a pokusy o zneužití platebních karet a bankomatů se naopak neustále množí. Vysvětlení je jednoduché – riziko dopadení, teoretická výše výtěžku i náklady na provedení jsou u těchto novějších typů kriminality výrazně nižší. Tomuto fenoménu se blíže věnuje následující exkurz a následující kapitola o kyberbezpečnosti.

Zdroj: PČR, idnes.cz, tyden.cz

Exkurz

Fenomén skimmingu

Skimming (z anglického slova Skimming – sbírání dat) se v posledních letech stal závažným ohrožením celého spektra obyvatelstva, využívajícího služeb bankomatů. Jedná se o jeden ze způsobů zjišťování PIN kódu během běžného použití bankomatu. Klíčové pro získání informací z kreditních karet jsou tzv. skimmovací zařízení, která jsou obvykle nainstalována přímo do otvoru pro kartu v bankomatu. Obvykle se skládají z dvou částí, kdy každá má diametrálně odlišnou funkci. Jedna část dokáže načíst data z magnetického kroužku karty při jejím vložení do bankomatu, známé jako „skimmovací hrdlo“, zatímco druhá část⁷, tzv. skimmovací lišta, slouží k získání, respektive rozpoznání PIN kódu dané karty. Celé toto zařízení má „splynout“ s bankomatem, aby došlo k jeho přehlédnutí a uživatel pachateli fakticky „odevzdal“ svou kartu, včetně bezpečnostního hesla.

Vzhledem k početnímu nárůstu této kriminality v posledních letech začala Česká spořitelna využívat tzv. antiskimmovací zařízení, které mělo zamezit možnost načítání informací

⁶ V roce 2012 bylo z celkové škody 11 milionů, způsobené finančním institucím, podařilo policii zpětně dohledat ¼ z této sumy.

⁷ Například upravená klávesnice, či minikamera.

z kreditních karet. Nicméně již v roce 2009 bylo toto zařízení poprvé překonáno. V roce 2012 poté došlo k raketovému nárůstu odhalených pokusů o skimming, z 85 případů, evidovaných v roce 2011, na 150 v roce 2012. Drtivá část této trestné činnosti se odehrála na území hlavního města Praha (114 případů) a v Plzni (10 případů⁸), skimming byl dále odhalen i na území měst Olomouc, Brno, Kroměříž a Vyškov.

Pachatelé, dopouštějící se této trestné činnosti, se zaměřují především na zahraniční banky, respektive klienty zahraničních bank, navštěvující naše území. V současné době je deklarováno, že pachatelé si vybírají výhradně bankomaty uvnitř, případně poblíž finančních institucí, aby nabudili u obětí stav určité „jistoty“. Zařízení jsou na bankomaty instalována výhradně v časných ranních hodinách z pátku na sobotu, jelikož se spoléhají na fakt, že zablokování karty zahraničními klienty bank je možné provést až v průběhu pracovních dnů a zůstává tedy dostatek času na provedení samotné krádeže. Nelegální výběry z účtů jsou poté prováděny většinou z mimoevropských zemí, případně Bulharska a Ukrajiny.

Pachatel mnohdy nemusí být k extrakci informací fyzicky přítomen, po instalaci zařízení již veškerý informační přenos probíhá bezdrátově. Zpravidla poté dochází k odčerpávání peněz mimo území České republiky a to za služby v zahraničí.

Pachatelé skimmingu jsou na území České republiky v 99 procentech případů obyvatelé Rumunska a Bulharska, nicméně byly zjištěny i případy propojení českých státních příslušníků s tímto druhem trestné činnosti. Existuje všeobecně uznávaný předpoklad, že tito pachatelé přijíždějí do České republiky pouze s cílem páchaní trestné činnosti a po jejím vykonání se vrací zpět domů. Díky tomuto přístupu má skimming charakter organizované trestné činnosti, páchané na mezinárodním poli, se sofistikovanou strukturou, která zajišťuje funkčnost skupiny. V případě zadržení jejich jednotlivých členů existuje minimální šance na další postup v rámci ničení těchto organizovaných skupin, především díky jejich neochotě spolupracovat a existenci mimo území České republiky.

Jeden z nových trendů kriminality, týkající se bankomatů, již nefunguje na bázi extrakce informací z karet uživatelů, ale na přímé krádeži vybraných financí. Pachatel instaluje na bankomat hliníkovou krytku, která sice dovolí výběr, nicméně brání vydání peněz po zadání výběru. Očekává poté, že poškozený se v panice bude snažit vyhledat pomoc v bankovním institutu a zanechá bankomat, včetně domněle nevybrané finanční sumy, nechráněný. Pachatel poté pouze odejme krytku a tím připraví oběť o hotovost výběru. Tento model částečně připomíná jednu ze starších metod skimmingu, tzv. libanonskou smyčku, která spočívala v zablokování karty v bankomatu. Proto poskytovatelé bankovních služeb důrazně doporučují za žádných okolností neopouštět bankomat, ani v případě „poruchy“ a kontaktovat banku prostřednictvím telefonu, uvedeného na bankomatu.

V letošním roce bylo v České republice evidováno několik desítek případů odhalení skimmovacího zařízení v bankomatech. Nejčastěji se jedná o velká města – Brno, Břeclav, Karlovy Vary, České Budějovice atd. Peníze pak byly vybírány v Severní i Jižní Americe či v Asii. Nejvíce případů hlásí za první pololetí tohoto roku jižní Morava. Zatímco loni došlo ke zjištění 4 případů instalace skimmovacího zařízení, za první 3 měsíce letošního roku bylo evidováno již 16 případů. Fenomén se po republice rozšířil z Prahy, kde byl rozšířen před několika lety. Objasněnost případů je však v Praze přes 50 procent, přičemž loni se podařilo odhalit šest skupin, ve kterých 'pracovalo' 13 lidí. Vyšetřovatelé jim přičetli škodu zhruba 18 milionů korun, které se údajně pokusili odčerpat z účtů. Letos policisté dopadli tři gangy, všechny pachatele zadrželi při činu. Právě vysoká úspěšnost boje s tímto fenoménem zapříčinila jeho rozšíření do dalších měst po ČR. Bližší informace k jednotlivým případům nalezne čtenář v následující kapitole věnující se vybraným událostem ve sledovaném období.

Zdroj: cybersecurity.cz, policista.cz, policie.cz, mesec.cz

⁸ Na území města Plzně poté došlo v průběh prvního kvartálu roku 2013 k odhalení dalších 5 skimmovacích zařízení

Leden

Německo převez domů 674 tun zlata z New Yorku a Paříže

Německo se chystá postupně přesunout polovinu svého zlata uloženého v New Yorku do trezorů Bundesbanky ve Frankfurtu. Celkem půjde o 300 tun kovu. Dalších 347 tun zlata chtějí Němci přesunout domů z Paříže. Německé zlato se v zahraničí ocitlo během studené války, kdy se je tehdejší západoněmecká vláda snažila uložit co nejdále na západě pro případ sovětského útoku.

Důvody pro uložení části jeho zlatých rezerv ve finančních centrech jako Londýn či New York ale podle newyorského listu přetrvávají. V případě měnové krize je díky tomu lze rychle umístit na trh pro obnovení důvěry.

V New Yorku má Německo zlato uložené v tamní pobočce americké centrální banky. Stejně jako další země, které tam svůj žlutý kov skladují, za to nic neplatí. Američané se domnívají, že přítomnost cizích rezerv v podzemním trezoru newyorského Fedu

podporuje status dolaru jako celosvětové rezervní měny.

Němci se pro návrat zlata rozhodlo po loňské veřejné debatě o rezervách a parlamentním sporu o to, zda Bundesbanka má o svých rezervách v zahraničí skutečně přehled a zda je má pod kontrolou. V Německu se mimo jiné objevily spekulace, že jeho zlato v USA někam zmizelo, anebo že je nahradila méně kvalitní slitina. Bundesbanka takové spekulace odmítá, veřejnému tlaku ale nakonec ustoupila. Přesun zlata by chtěla dokončit do roku 2020. Podrobnosti o něm nechce z bezpečnostních důvodů prozrazovat.



Čtveřice mužů podle policie vyvedla ze země 204 milionů z kauzy Edbusy

Kriminalisté z protikorupčního útvaru obvinili z podílnictví čtveřici mužů, která se podle nich obohatila o 204 milionů. Peníze patřily známé firmě Edbusy, která svými "výhodnými" úvěry připravila o úspory tisíce lidí. Obvinění muži se dostali do vedení společnosti a podle policistů vyvedli peníze do zahraničí.

Podle závěrů kriminalistů převzala čtveřice mužů pravomoci k řízení brněnské akciové společnosti Edbusy v polovině roku 2008. Následně dohodli s další společností se sídlem v Londýně, kterou však sami ovládali, kontrakt týkající se ověřování klientů Edbusy.

"Přestože k žádným prokazatelným plněním smlouvy nemělo docházet, londýnské společnosti bylo bankovními transakcemi převedeno asi 4,3 milionu eur," sdělil mluvčí Útvaru pro odhalování korupce a finanční kriminality Jaroslav Ibehej.

Další podobné aktivity jim koncem roku 2008 překazili kriminalisté. Ti totiž zadrželi dvě hlavní tváře společnosti - Martina Žouželku a Lukáše Příbyla - a následně obstavili finance Edbusy.

Čtveřice podnikavců záhy přišla s další fintou, jak peníze vyvést ze země. "Londýnská společnost uplatnila pohledávku ve výši asi 3,7 milionu eur za neuhrazené služby. Následovalo rozhodčí řízení v Německu, které skončilo ve prospěch britské společnosti," popsal Ibehej.

Zřejmě proto, aby se zamezly stopy, prodala se pohledávka v roce 2009 společnosti se sídlem na Seychelách. Po několika měsících ji pak koupila jiná britská obchodní společnost, kterou však opět ovládala čtveřice obviněných. "Ta následně v České republice v rámci exekučního řízení dosáhla výplaty asi 93,6 milionu korun," dodal mluvčí.

Svým jednáním si muži podle kriminalistů přišli zhruba na 204 milionů korun. Policistům se podařilo zajistit majetek, převážně nemovitosti, v hodnotě asi dvacet milionů korun, který si podle Ibeheje pořídili z výnosů z trestné činnosti.

Jeden z obviněných je v současné době ve vězení za jinou trestnou činnost, další muž skončil ve vazbě a zbylí dva jsou stíháni na svobodě. Všem hrozí trest od tří do osmi let vězení.

Lupiči si z přepadené dodávky odnesli přes dva miliony korun

Lupiči, kteří přepadli ve Velkých Popovicích dodávku s penězi, si z ní odnesli více než dva miliony korun. Přepadený vůz patřil společnosti G4S a zřejmě vezl peníze do bankomatu, který je umístěn hned u brány blízkého pivovaru.

Únor

Nizozemská vláda musela znárodnit čtvrtou největší banku

Nizozemská vláda znárodnila bankovní a pojišťovací společnost SNS Reaal NV, která je čtvrtou největší bankou v zemi. Náklady státu na záchranu banky mají činit 3,7 miliardy eur (95 miliard Kč). SNS Reaal obdržela již v roce 2008 od státu 750 milionů eur. Operace banky byly převážně ziskové, avšak klesla hodnota realitního majetku v jejím držení, což oslabilo rozvahu banky natolik, že se ocitla pod limitem solventnosti.

Banka v poslední době stále častěji varovala, že má problémy, a jednala s několika soukromými subjekty o svém převzetí. Podle ministra bylo však znárodnění pro budoucnost banky nejlepší možností.

O koupi části SNS uvažovaly tři největší banky v Nizozemsku - ING, ABN Amro a družstevní Rabobank. Evropský regulátor však zablokoval prodej ING a ABN, protože i tyto banky byly znárodněny a získaly pomoc od státu.

Všechny tři banky však budou požádány, aby přispěly k záchraně SNS celkem jednou miliardou eur. V rámci nizozemského systému si drobné retailové banky v zemi navzájem pojišťují své vklady.



Bankomaty v Brně kopírovaly platební karty, stopy vedou do Kalifornie a na Tchaj-wan

Do bankomatu u pobočky České spořitelny v Panské ulici v Brně někdo na začátku února namontoval techniku, která kopírovala platební karty. Policie a banka zatím vědí o dvou poškozených klientech, může jich však být víc. Jednomu z nich z účtu někdo "vyluxoval" zhruba dvacet tisíc. Stopy v tomto případě vedou do Kalifornie.

Záhy se však ukázalo, že napadených zařízení je několik. "Techniku na takzvané skimmingování namontovali pachatelé na různé bankomaty v centru města na ulicích Česká a Masarykova," informovala policejní mluvčí Petra Vedrová.

Ohroženi jsou i lidé, kteří vybírali peníze z bankomatů v Břeclavi. I tam neznámí podvodníci kopírovali karty. Peníze z účtů poté několika lidem zmizely na Tchaj-wanu. Není to však první případ skimmingu v Břeclavi, ten se udal již v červenci roku 2010.

Lupiči pálili na auto s penězi bez varování

Trojice maskovaných lupičů přepadla vůz agentury Loomis převážející zhruba 33 milionů korun na doplnění do bankomatů. Incident se stal v Přemyslovicích na Prostějovsku. Vůz vyjel z olomoucké centrály České spořitelny.

Svým autem vůz donutili zastavit a poté vystoupili a bez varování zahájili palbu ze samopalu a brokovnice. Stříleli přitom i ve směru mezi domy. Auto první nápor vydrželo, útočnickům se však střelbou podařilo vyřadit motor, tudíž posádka obrněného vozu nemohla ujet, o což se zprvu pokoušela.

Lupiči ji nakonec donutili z auta vylézt pod hrozbou použití granátu. Pak přeházeli do svého vozu schránky s penězi, zapálili na silnici hořlavinu a ujeli. Podle ředitele firmy Loomis bylo přepadení na české poměry poměrně brutální. Podle zástupců společnosti byli pachatelé na přepadení velmi dobře připraveni a pravděpodobně měli kvalitního informátora.

Útoky na internetové bankovníctví ČSOB, Komerční banky, České spořitelny a Raiffeisenbank

Trojici největších tuzemských bank, ČSOB, Komerční banka a České spořitelně, a Raiffeisenbank nefungovalo dne 6. 3. 2013 internetové bankovníctví a stránky. Mluvčí Komerční banky Monika Klucová potvrdila ČTK, že banka čelila tzv. DDoS útoku. K úniku clientských dat nedošlo, uvedla. Internetové stránky nefungují ani pražské burze. V provozu nejsou stránky energetické burzy, burzy cenných papírů a centrálního depozitáře, řekl ČTK mluvčí burzy Jiří Kovařík.

I podle mluvčího Raiffeisenbank Tomáše Kofroně to vypadá na útok hackerů. 'Internetové bankovníctví přestalo fungovat kolem 9:15. Příčinu zjišťujeme, podle dosavadních informací to ale vypadá na cílený útok,' uvedl Kofroň.

Podle zjištění ČTK trojici největších bank nefungují zhruba od 9:00 vedle internetového bankovníctví ani internetové stránky a elektronické bankovníctví přes chytré telefony. Útokům hackerů v posledních dnech čelily i některé tuzemské zpravodajské servery. Rovněž v jejich případě, šlo o tzv. DDoS útoky. Ty uměle vyvolají přetížení sítě, kvůli němuž služba krátkodobě vypadá nebo se déle načítá.

Hackeri napadli web UniCredit Bank

"Unicreditgang: Vítejte na nových stránkách. S lítostí musíme oznámit, že se nám veškeré vaše peníze někam ztratily." Takový text umístila česká hackerská skupina na web banky UniCredit. Nešlo o zahlcení serveru jako při útocích minulý týden, ale skutečné hackerské proniknutí. Česká hackerská skupina Czechurity odstavila web tuzemské pobočky UniCredit Bank. Šlo o krátký pětiminutový výpadek, poté web normálně fungoval.

Útok nebyl veden pomocí DDoS útoků, tedy přetížení serveru velkým množstvím dotazů, ale jednalo se o skutečné hackerské proniknutí. Další bankovní systémy UniCredit Bank údajně napadeny nebyly. O tom, že se nejednalo o DDoS útok, informovali sami hackeři z Czechurity: „DDoS? Ne, děkujeme. Preferujeme skutečné umění,“ stálo na hacknutém webu.

V daném případě velké umění nebylo třeba kvůli až neuvěřitelné neopatrnosti administrátora.

Čeští hackeři už 26. února upozorňovali, že „něco“ chystají. Podle serveru je možné, že se hackeři chystají také k dalším krokům. Na napadeném webu totiž informovali o tom, že na Twitteru zveřejní další informace. Hackeři z Czechurity už dříve napadli servery společnosti CS Link a zveřejnili i databázi zákazníků společnosti.

Sberbank chce do roku 2016 zdvojnásobit tržní podíl v ČR. Cílí na Rusy a firmy obchodující v Rusku

Sberbank oficiálně uvedla svoji značku na český a evropský bankovní trh. Třetí největší banka v Evropě, funguje v České republice pod značkou Sberbank CZ od konce února. Vznikla po úspěšné akvizici Volksbank International v loňském roce. Česko chce banka využít jako odrazový můstek pro další mezinárodní expanzi.

„Jsme jediná ruská banka v ČR, jsme proto jedinou jasnou volbou pro firmy obchodující s rusky mluvícími zeměmi,“ řekl na středěční tiskové konferenci banky Herman Gref, generální ředitel a předseda představenstva Sberbank Rusko.

Sberbank se chce zaměřit na financování rusko-českých obchodů. Zároveň hodlá podpořit ruské investice v Česku. Po roce od dokončení akvizice Volksbank proto podnikla další krok k podpoře českého exportu a podepsala memorandum o vzájemné spolupráci s Českou exportní bankou.

Sberbank vlastní bankovní síť v České republice po akvizici poboček Volksbank. Dohoda o prodeji banky byla podepsána v únoru roku 2012, pod značkou Sberbank vystupuje banka na českém trhu od konce letošního února. Při této příležitosti otevřela již pod značkou Sberbank novou vlajkovou pobočku v ulici Na Příkopě v Praze.



Kromě rozsáhlých investic do rekonstrukce poboček v Česku, které by se měly pohybovat v desítkách milionů Kč, si banka stanovila za cíl přinést do bankovníctví další technologické inovace. V dubnu pak představí upravené produkty a služby, kterými chce oslovovat klienty.

Duben

Banka v kapse zažívá boom. Už čtvrt milionu Čechů ovládá účty z chytrých mobilů

Přes 410 tisíc Čechů má banku v kapse. Respektive v mobilu, který mají v kapse (nebo kdekoli v jinde). Stáhli si totiž do svého chytrého mobilního telefonu aplikaci, která jim umožňuje kontrolovat zůstatky na jejich běžném účtu, zadávat platební příkazy či jakkoliv jinak spravovat jejich běžný účet. A přibližně čtvrt milionu uživatelů tak opravdu činí, jsou aktivní a posílají platby ze svého telefonu. Jejich počet navíc podle vyjádření bank průběžně roste, do konce roku by pak mělo přibýt dalších zhruba 160 tisíc uživatelů, kteří si aplikaci od své banky minimálně stáhli a jednou vyzkoušeli.

Využívání internetového bankovníctví prostřednictvím mobilního telefonu s sebou přirozeně nese také mnohá rizika. O těch bude blíže pojednáno v následující kapitole věnující se problematice kybernetické a informační bezpečnosti.

Slováci lapili zloděje, kteří z bankomatů ukradli 1,7 milionu eur

Slovenská policie chytila zloděje, kteří ze třinácti bankomatů vykradli celkem 1,7 milionu eur, tedy v přepočtu zhruba 45 milionů korun. Informoval o tom policejní prezident Tibor Gašpar.

Gašpar upřesnil, že policie zatím vznesla obvinění proti třem lidem, kteří zůstávají ve vyšetřovací vazbě. Zloději se podle něho pokusili minulý týden v noci ze čtvrtka na pátek vykrást ještě čtrnáctý bankomat, ale to se jim nepodařilo.

"Je jisté, že byly použity kopie originálních klíčů, které jdou do bankomatu. Pachatelé rovněž znali trezorové kódy i kódy od alarmů, jež chránily prostory, v nichž jsou bankomaty umístěny," sdělil dále Gašpar.

Zloděje zadržela při kontrole policejní hlídka, které se nezdál jejich vůz. Lidé ve vozidle se snažili vypadat jako pracovníci bezpečnostní agentury, ale policisté si všimli, že auto není patřičně označeno. Při následné prohlídce našli kazety z čerstvě vykradeného bankomatu, v nichž bylo 200 tisíc eur. Navíc zjistili, že vozidlo bylo vybaveno zařízením k automatickému otáčení registrační značky.



Policisté chytili u bankomatu v Brně Bulhara, který kopíroval kreditky

Jihomoravským kriminalistům se podařilo o víkendu chytit cizince, který na bankomat v centru Brna namontoval skimmovací zařízení. To kopírovalo údaje z platebních karet. Poškozeným lidem pak někdo vybral z účtu peníze v zahraničí.

"Díky bleskové reakci policistů byl podezřelý muž dopaden těsně poté, co přišel k bankomatu, skimmovací zařízení odstranil a chystal se nerušeně odejít," uvedla mluvčí jihomoravské policie Petra Vedrová.

Kriminalisté pak prohlédli i hotelový pokoj, kde byl jednatřicetiletý občan Bulharska ubytovaný. Našli tam zařízení umožňující kopírování dat z platebních karet.

"Cizinec už byl obviněn z trestného činu neoprávněné opatření, padělání a pozměnění platebního prostředku, a je stíhán vazebně. Prozatím byl obviněn ze spáchání dvou skutků, v nejbližší době bude jeho trestní stíhání rozšířeno o další," doplnila mluvčí.

Podvodníci kopírovali ve Varech platební karty, peníze vybrali v Peru

Karlovarští kriminalisté hledají dva muže, kteří díky kopírovacímu zařízení na jednom z bankomatů v lázeňské části města padělali platební karty. Vyrobili jich nejméně šest. Tisíce korun díky tomu pak někdo v dubnu vybral v Peru.

"Dle kurzovního lístku došlo k výběru částky ve výši 24 tisíc korun. Celková škoda je však vyšší, 102 tisíc korun," vyčíslila policejní mluvčí Kateřina Böhmová.

Kriminalisté nyní pátrají po obou mužích, které zachytily kamery bankomatu. Podle policistů je možné, že jde o cizince.

V Evropě dle studie přibývá zařízení, která kradou údaje z karet

V Evropě přibývá nelegálních zařízení, která při nákupu benzínu nebo jízdenek kradou údaje z bankovních karet. Vyplývá to z průzkumu mezinárodní organizace European ATM Security Team (EAST), o kterém informoval britský zpravodajský server BBC. Nárůst počtu těchto čteček, instalovaných v automatech na jízdenky, zaznamenalo pět z 23 evropských zemí.

Ve dvou zemích se zvýšil počet případů, kdy se čtečky nacházely v parkovacích hodinách. V šesti zemích je zaznamenali v samoobslužných čerpacích stanicích.

Čtecí zařízení, která kradou údaje z bankovních karet, podvodníci častěji umísťují do bankomatů.

Organizace EAST v březnové zprávě neuvedla, kterých států se nárůst nelegálních čteček týkal. Informace o podvodech s kartami společnosti poskytly například Francie, Německo, Rusko nebo Británie.

Květen

Kamera zachytila podvodníka, jak v Budějovicích upravuje bankomat

Už na čtvrtém bankomatu v Českých Budějovicích odhalili policisté za poslední dva měsíce skimmovací zařízení. Policisty na skimmovací zařízení upozornil všímavý občan, který poznal, že bankomat není v pořádku.

Podobu muže, který tam zařízení namontoval, zachytila kamera umístěná na přístroji. Další skimmovací zařízení objevila policie v Českých Budějovicích v březnu na bankomatech v ulici Krajinská, Jeronýmova a na Senovážném náměstí. Totožnost dvou pachatelů se policistům podařilo už odhalit.

Kriminalisté apelují na občany, aby byli při výběru peněz z bankomatů velmi opatrní. "V případě, že budete mít problémy se zastrčením karty, tak ji dovnitř netlačte násilím, ale okamžitě kontaktujte policii či správce bankomatu. Může se totiž stát, že právě na tomto bankomatu je skimmovací zařízení nainstalované," apelovala mluvčí.

Izraelec nedostal peníze z bankomatu, zastřelil čtyři lidi i sebe

Přestřelka se odehrála v dopoledních hodinách místního času v bance Hapoalim ve městě Beerševa. Muž, kterého místní média označila jako bývalého hraničního policistu, nejprve do banky přišel s žádostí o půjčku. Vzhledem k dluhům mu ji však peněžní ústav odmítl dát.

Izraelec při odchodu zamířil k bankomatu a pokusil se vybrat nějakou hotovost. To se mu však také nepodařilo. Vrátil se zpět do banky a začal střílet do lidí. Zastřelil jednoho pracovníka za přepážkou a tři klienty banky. Podle svědků citovaných agenturou Reuters se dokonce k jednomu sehnul a zkušel jeho tep, aby se ujistil, že je oběť vskutku mrtvá.

V USA sedm hackerů inkasovalo z účtů 45 milionů dolarů

Za jednu z největších online bankovních loupeží označují američtí vyšetřovatelé akci mezinárodní skupiny hackerů, kteří s využitím ukradených údajů z debetních karet odčerpali během několika hodin z bankovních účtů až 45 milionů dolarů. Sedm pachatelů v New Yorku americké úřady zatklly a obvinily z bankovní loupeže.

Hackeři si za cíl vybrali dvě banky ve Spojených arabských emirátech a v Ománu, sdělili novinářům představitelé amerického ministerstva spravedlnosti. Z bankomatů získali peníze

prostřednictvím 40 500 výběrů ve 27 zemích. Všichni zadrženi jsou američtí občané z města Yonkers nedaleko New Yorku. Osmý obviněný a vůdce bandy Alberto Yusi Lajud-Pena se koncem dubna v Dominikánské republice stal obětí vraždy. Není zatím známo, zda tento zločin s bankovními krádežemi souvisí.

K nezákonným výběrům došlo loni v prosinci a letos v únoru, uvedli američtí prokurátoři. Hackeři se dostali na servery společností, které zpracovávají finanční transakce držitelů debetních karet. Odblokovali limity pro jednorázový výběr a s pomocí ukradených identifikačních kódů se zmocnili uložených peněz. Získané prostředky se snažili "vyprat" nákupem luxusního zboží.

Útok hackerů na servery justičních orgánů

Servery justičních orgánů amerického státu Washington napadli hackeři, kteří se podle správců systému mohli zmocnit až 160 tisíc čísel sociálního zabezpečení a milionu čísel řidičských oprávnění. Získané údaje jsou v USA považovány za velmi citlivé, protože s jejich pomocí mohou zločinci založit v bance účet, získat bankovní úvěr, žádat o daňové výhody či si zajistit falešnou identitu. Útok byl zjištěn už v únoru, ale správci serveru se tehdy domnívali, že hackeři přístup k citlivým osobním údajům nezískali. Vyšetřovatelé ale později zjistili, že 94 čísel sociálního zabezpečení bylo zneužito a ostatní mohla být ukradena. Majitelé zneužitých dat byli podle policie varováni.

Červen

Microsoft odhalil síť napadených počítačů okrádajících uživatele

Microsoft odhalil síť několika milionů napadených počítačů, které okradly uživatele o víc než půl miliardy dolarů (asi deset miliard korun). Stál za nimi škodlivý program Citadel šířený s nelegálními kopiemi Windows XP. Oznamovala to společnost Microsoft.

Napadené počítače umožnily zločincům ukrást podle odhadů deset miliard korun tím, že řídicím serverům odesílaly informace o uživatelských jménech a heslech pro přístup k on-line bankovníctví. Americká FBI a policie v několika desítkách zemí odpojily servery, ze kterých zločinci napadené počítače ovládali.

Microsoft se na škodlivý software Citadel zaměřil poté, co vyšlo najevo, že pro své šíření používá pirátské verze Windows s podvodně získanými licenčními klíči. Část lidí ani nemusela vědět, že instaluje nelegální kopii. S postupem času Citadel začal využívat i komplikovanější způsoby, jako jsou podvodné e-maily lákající uživatele ke spuštění přílohy nebo napadení legálních webových stránek a přesměrování uživatelů na stránky se škodlivým softwarem.

Vyšetřovatelé Microsoftu zjistili, že kromě autora softwaru Citadel, který je známý pouze pod přezdívkou Aquabox, se na správě celého systému podílelo dalších 81 podezřelých.

Citadel je velice propracovaný škodlivý kód, který si mohou lidé napojení na komunitu internetových zločinců pronajmout za měsíční poplatek v řádu desítek tisíc korun. Autor malwaru svůj produkt v průběhu několika měsíců neustále vylepšoval tak, že například v novějších verzích uživatelům podsouval falešné stránky pro přihlášení k bankovním účtům na webech finančních ústavů a napadeným počítačům bránil v aktualizaci antivirových systémů. Chránil se tak před případným odhalením.

Evropská komise chce po bankách víc údajů o klientech pro boj s daňovými úniky

Evropská komise navrhla zvýšit rozsah informací, které musejí banky o svých klientech poskytovat úřadům v Evropské unii. Tento krok má pomoci v boji s daňovými úniky, kvůli kterým členské země unie přicházejí ročně až o bilion eur (tedy v přepočtu téměř 26 bilionů korun).

Banky by podle návrhu měly poskytovat například údaje o zůstatcích na účtech, dividendách a kapitálových příjmech klientů. "Členské státy tak budou lépe vybaveny pro výběr daní," uvedl evropský komisař pro daňové záležitosti Algirdas Semeta. "Bude to další mocná zbraň v našem arzenálu pro boj s daňovými úniky," dodal.

Návrh komise ale pravděpodobně narazí na odpor ze strany Lucemburska, které nechce přikročit k většímu uvolnění bankovního tajemství, než k jakému přistoupilo sousední Švýcarsko. Lucembursko již sice podepsalo dohodu o výměně informací o bankovních účtech od roku 2015, představitelé země se však staví zdrženlivě k tomu, jaký typ údajů budou ochotni poskytovat.

České banky by zvládly i další krizi, ale pozor na kampeličky, vyplývá z testů ČNB

Tuzemské banky jako celek jsou podle výsledků zátěžových testů, které provedla Česká národní banka, nadále odolné vůči případnému nepříznivému vývoji. Celková stabilita sektoru by neměla být ohrožena ani při výrazně špatném vývoji ekonomiky. Vyplývá to ze Zprávy o finanční stabilitě, kterou zveřejnila ČNB. Výsledky jsou tak podobné předchozím testům, které ČNB provedla.

Rovněž sektor pojišťoven vykázal podle testů ČNB díky vysokému kapitálovému polštáři dostatečnou míru odolnosti vůči nepříznivému vývoji. Sektor penzijních fondů zůstává citlivý na rozkolísanost cen držených cenných papírů. "Navýšení kapitálu v průběhu roku 2012 však jeho odolnost ve srovnání s minulým rokem posílilo," uvedla ČNB.

"Bankovní sektor je stabilní a odolný, avšak rizika pro další vývoj spatřujeme zejména v případě pokračování nebo dokonce prohlubování ekonomické recese. Na finančních trzích pak vidíme určitá rizika spojená s honbou za výnosem," uvedl guvernér ČNB Miroslav Singer.

Zdroj: idnes.cz, ihned.cz, bankovnictvi.ihned.cz

INFORMAČNÍ TECHNOLOGIE A KYBERNETICKÁ BEZPEČNOST

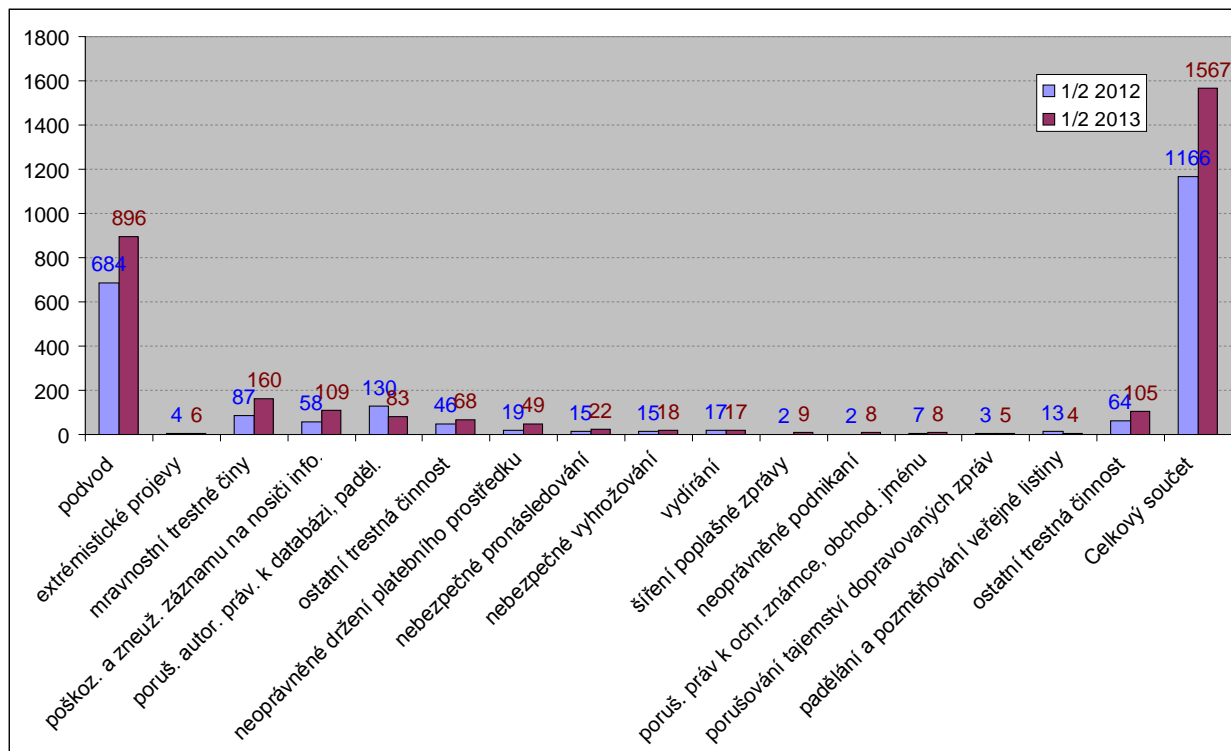


Policejní statistiky a jejich interpretace

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.

V níže uvedeném grafu je patrná skladba trestných činů v oblasti informační kriminality za první pololetí roku 2013 a zároveň jsou v grafu uvedena data za první pololetí roku 2012 pro komparaci.



Zdroj: PČR

Z výše uvedeného grafu je patrné, že fenomén informační kriminality nadále sílí – došlo ke zvýšení počtu trestných činů zjištěných na internetu a to o více než 400 případů. Zvýšil se také počet podvodů na internetu. Počet evidovaných mravnostních trestných činů na internetu se stejně jako trestný čin poškození a zneužití záznamu na nosiči informací téměř zdvojnásobil.

V oblasti porušování autorských práv nadále dochází k přesunu trestné činnosti z původně dominantního prostředí výměnných sítí do segmentu datových úložišť, přičemž pro výměnu odkazů a případně hesel ke komprimovaným materiálům s obsahem autorsky chráněných děl, šířených v rozporu s autorským právem, jsou využívány tematická fóra a diskuse. Celý segment se rozdrobil do velké masy drobných útoků, což znemožňuje účinný postup proti takovému jednání. Současně je patrná technická propracovanost tematického dohledávání v rámci samotných úložišť, což umožňuje tyto masivně využívat i jako samostatný fulltext pro dohledání zejména multimediálního obsahu bez potřeby využití propojení s jinými linky.

Internet resp. prezentace jsou na našem území prezentovány poměrně obezřetně a většinou nekolizně ve vztahu k protiprávnímu jednání ze strany tzv. extremistů a extrémistických hnutí. Extremisté k důraznějším a extrémněji laděným projevům a ke komunikaci již využívají uzavřených komunit a to s dominantním zapojením sociálních sítí. To co je však sledovatelné je aktuální radikalizace běžných uživatelů sítě internet, kteří se nechávají strhnout k extrémistickým a xenofobiím projevům a poznámkám v diskusích pod články v internetových zpravodajstvích. Rovněž tak, pokud jsou zcela zjevné protiprávní útoky v této oblasti, pak tyto se objevují téměř výhradně v jurisdikcích resp. tzv. hostingu v zahraničí, kde takové projevy nejsou postihovány a to zejména v USA.

Na neustálém vzestupu jsou stále útoky formou tzv. phishingu (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, tj. útokem vytvořených cílových stanic, určených přes rozličné architektury sítí k páčání dalších kriminálních aktivit. Na našem území nebyl zjištěn výskyt organizátorů takového jednání, nicméně často se vyskytují 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. V hodnoceném období jsou neustále zaznamenávány snahy o umístění phishingových stránek. Ze stávajících poznatků lze pak upozornit na úsilí, místo shora uvedené aktivity tzv. bílých koňů, realizovat vytváření elektronických obchodů, které budou vytvářeny primárně za účelem krytí zdrojů a původu financí pocházejících z trestné činnosti zejména z phishingových útoků a zneužitých čísel platebních karet.

V souvislosti s projevy pachatelů, zejména podvodných jednání, je na vzestupu skrývání své činnosti za cíleně vznikající společnosti, kde jejich struktura a vnitřní chod je stavěn tak, aby nebyla možná konkrétní identifikace proběhlých transakcí. Obdobně jsou kryty i finanční transakce.

V rámci elektronického obchodování se ve větší míře projevilo v minulém období trend sofistikovaného vytváření elektronických virtuálních obchodů, kde je realizováno v krátkém údobí velké množství obchodů, přijetí objednávek, jsou realizovány platby, ale dále se již nerealizovalo dodání objednaného zboží. Na závěr docházelo a dochází k zániku aktivit obchodu bez dalších reakcí. Rovněž tak jsou detekovány výskyty krádeží identit, které jsou zneužívány, ať už ke kompromitaci faktických subjektů a nebo využití jejich identity jako legendy pro páčání zejména podvodných jednání. Nezanedbatelné jsou podvodné aktivity v rámci aukčních portálů, kde se mimo podvrhy objevují masivně i věci pocházejících z trestné činnosti a věci, jejichž volná distribuce není povolena.

Novým prvkem je opětovné rozšíření podvodných aktivit spočívajících výhradně na sociálním inženýringu s absencí technologického využití útoku.

V rámci šíření zakázaných forem pornografie je stále patrné, že dochází k vytváření a profesionalizaci uzavřených komunit, které se neustále zdokonalují v prověřování svých členů. Dané materiály jsou pak šířeny s větší latencí a to zejména přes elektronickou poštu, úložný prostor a přes přímou výměnu instant messengerů. Detekce takových aktivit vyžaduje větší nasazení vlastní agenturní činnosti, aby byla možná infiltrace do daných komunit. Nově se objevuje, v souvislosti s dětmi, snaha pachatelů získávat cestou sítě Internet materiály intimního až pornografického charakteru, zejména fotografií, přímo od dětí. V tomto ohledu to vypovídá

o profesionalizaci pachatelů, kteří využívají taktiku sociálního inženýringu. Pachatelé si vyhledávají oběti zejména v prostředí chatů a sociálních sítí. Také jsou viditelné projevy, kde samotné děti samy cíleně nabízejí jimi samotnými vytvořené materiály charakteru dětské pornografie za peníze či benefity, především dobytí kreditu mobilu.

To co je s rozšiřující platformou zejména sociálních sítí a tematicky zaměřených aplikací na okolí samotných uživatelů patrné, je růst využití resp. zneužití informací získaných k jednotlivým uživatelům, čehož následně je zneužíváno ke kriminálnímu jednání, kdy dané osoby jsou tzv. na míru kompromitovány a rovněž je u nich využita znalost soukromí k působení na ně.

Pokud se týká rizik vyplývajících ze znemožnění zjištění identit pachatelů, je nutné poukázat na nebezpečí šíření anonymního připojení do Internetu prostřednictvím volně přístupných Wi-Fi bodů a anonymního připojení z předplacených karet mobilních operátorů. Specifickou a stále více využívanou technologií k páčání trestné činnosti jsou pak anonymizační sítě a botnetové sítě.

Bezprostředně lze v oblasti informační kriminality očekávat sledování technologických trendů. Tak jako roste poměr počtu mobilních zařízení a význam zpracovávaných dat v těchto mobilních zařízeních, tak bude narůstat i šíření mobilního malware a budou se množit útoky na tyto zařízení více než doposud. Zcela jistě lze očekávat celosvětově, a to i u nás, projevy nesouhlasu s politickými a jinými veřejnými názory, na něž vzniknou reakce formou hackerských útoků. Profesionalizace pachatelů informační kriminality bude mít stále větší míru propracovanosti s jasnější dělbou jednotlivých rolí. Větší bude i zapojení tzv. botnetových sítí, které mají za úkol anonymizovat aktivitu původce nelegálního jednání a současně zvyšovat masivnost či technologickou koordinaci útoku. Během minulého roku, který lze zcela jasně definovat jako zlomový ve využívání tzv. cloudových řešení, které řeší vzdálená úložiště a správu dat, lze předpokládat větší míru útoků na takto centralizovaná data, kdy v případě prolomení ochrany bude docházet k masivnějším únikům informací, než tomu bylo doposud. Nové technologie nabízejí a stále více budou nabízet i větší možnosti pachatelů veškeré trestné činnosti zastírat vzájemnou komunikaci či výměnu dat s využitím právě nových služeb v informačních technologiích.

Zdroj: PČR

Zákon o kyberbezpečnosti

Dne 28. června 2013 předložil Národní bezpečnostní úřad vládě České republiky návrh zákona o kybernetické bezpečnosti a to se 2 rozpory s Ministerstvem vnitra.

Předložený materiál byl vypracován na základě usnesení vlády České republiky ze dne 30. května 2012 č. 382 k návrhu věcného záměru zákona o kybernetické bezpečnosti, kde bylo v bodu II. uloženo řediteli Národního bezpečnostního úřadu vypracovat návrh zákona o kybernetické bezpečnosti a předložit jej vládě do 31. července 2013.

Na přípravě zákona se podílelo také Ministerstvo vnitra a Ministerstvo obrany, Bezpečnostní informační služba, Úřad pro zahraniční styky a informace a Český telekomunikační úřad.

Očekávané bezpečnostní hrozby a trendy pro rok 2013

V posledním čtvrtletí 2012 došlo k takřka dvojnásobnému nárůstu mobilního malware ve srovnání s předchozím obdobím. McAfee tento fakt přiřazuje především ke skokovému nárůstu specifických oblastí malware.⁹

⁹ Jedná se například o Ransomware, Rootkits, Mac malware, Trojské koně se zaměřením na krádež hesel a Autorun malware.

Dle reportu organizace RSA se bude kyber kriminalita zaměřovat především na nové způsoby monetizace nefinančních dat, nárůst nových druhů finančního malware a nárůst hackerských útoků.

Ačkoliv počítačová kriminalita vykazuje určité známky zpomalení, dochází k větší sofistikovanosti útoků. Kybernetická kriminalita, hackerství a kybernetický boj prochází evolucí, jejíž hrozbě čelí celá paleta uživatelů informačních technologií.

V posledním kvartále 2012 identifikovali výzkumníci z McAfee následující trendy:

- **Kruh finančních podvodů rozšiřuje celosvětový rozsah:** Online finanční podvody se rozšířily celosvětově v 3. čtvrtletí roku 2012. Kyber zločinci využívají automatický systém přenosu (ATS), který byl původně využit při útoku na evropské finanční instituce¹⁰, a nyní se zaměřují na významné americké nadnárodní finanční instituce. Počítačová kriminalita je dnes založena na finančních výdělcích, jejich autoři spolupracují, což vede k ještě většímu ohrožení společností a uživatelů výpočetní techniky. V rámci potírání této kriminality policejní složky často naráží na neadekvátní a odmítavý přístup mnoha zemí, které tak tyto aktivity fakticky kryjí a mnohdy i využívají pro vlastní potřeby. Vyjma důrazu na zisk se množství kybernetických útoků orientuje také na manipulaci s daty oběti, případně přímo sabotáž výzkumných snah.
- **Pokračující vývoj Ransomware¹¹:** Počet zjištěných případů Ransomware narostl v 3. čtvrtletí o 43%, což z něj dělá jeden z nejrychleji rostoucích větví kyber kriminality.
- **Nárůst počtu zjištěného malware:** I když se nárůst v oblasti malware mírně zpomalil, celkový počet překročil 100 milionů vzorků. Mobilní malware takřka zdvojnásobil hodnoty z předchozího kvartálu, především prostřednictvím platformy Android¹². McAfee v současné době registruje více než 100 000 nových vzorků malware denně.
- **Historicky nejvyšší hodnota prolomených databází:** V 3. kvartále již došlo k překonání celkového množství průlomů databází, zaznamenaných v roce 2011. V roce 2012 došlo odhalení anebo tiché opravě takřka 100 s databázemi spojených nedostatků.
- **Rychlý nárůst skrytého malware:** Tento typ malware je považován za jeden z „nejhorších“, jelikož je navržen k tomu, aby jej nebylo možné detekovat. Tento druh malware je schopen se infiltrovat a napodobovat prostředí, což ho po nějakou dobu činí fakticky neodhalitelným. Mezitím slouží k čerpání citlivých dat, většinou bez možnosti zpětného vystopování.

Za několik set dolarů jakožto počáteční vklad a pár set měsíčně na poplatcích si může v dnešní době kdokoliv obstarat softwarové nástroje a zprovoznit vlastní botnetové centrum, které dovoluje nenápadně převzít kontrolu nad sítěmi počítačů, které poté slouží jako „zombie“, když jejich prostřednictvím dochází například k šíření malware.

Přichází tak nový způsob ochrany informací, kdy starý model, tedy silný perimetr a zabezpečení korporátního intranetu, nefunguje. V současnosti již není aktuální snaha zesílit vnější perimetr systému, ale snažit se odhalit případné útoky a chránit data. Fakticky se jedná o užívání kódování a aktivních procesů k monitorování známek neoprávněného vniknutí a extrakce informací.

Zdroj: mcafee.com, newsroom.cisco.com, csoonline.com

¹⁰ Viz. Operace High Roller.

¹¹ Jedná se o druh malware, který zablokuje přístup uživatele do systému a následně požaduje „výkupné“, za které bude systém odblokován.

¹² Nárůst mobilního malware z 350 000 útoků v roce 2012 na předpokládaný milion v roce 2013 je však stále nepatrný v poměru k útokům proti operačnímu systému Windows, který čelí v průměru 300 000 útokům denně.

Exkurz

Březnové hackerské útoky

První březnový týden se nesl ve znamení dosud nejintenzivnějších hackerských útoků v ČR. Nejprve byly napadeny servery iDNES.cz, iHNED.cz, Novinky.cz, Lidovky.cz a deník.cz. Menší vlna zasáhla i jiné weby, které však zaznamenaly pouze lehké problémy. Později téhož dne se útoky znovu opakovaly v plné síle a podlely jim i další weby jako Živě.cz, Mobilmania.cz nebo E15.

Distribuovaný útok (DDoS) je způsob, jak vyřadit server z provozu tím, že čelí vysokému počtu požadavků z více míst. "Počítače posílají nesmyslné požadavky, které zahlcují naše servery. Lidé se tak nemohou dostat na naše stránky. V tomto případě to byly statisíce požadavků za sekundu," shrnul podstatu problému programátor iDNES.cz Ivo Škola.

Za útokem stojí pravděpodobně botnet, tedy útočníky koordinovaná síť "zotročených" počítačů. Ty jsou napadeny virem, který útočnickům umožní využít jejich výkon - nejčastěji právě pro rozesílání spamu nebo DDoS útoky. Majitel napadeného počítače ani nemusí vědět, že jeho stroj na nějaký server útočí.

Podle posledních informací přišel útok z počítačů umístěných v Rusku. To ovšem neznamená, že samotným útokem stojí Rusové. Akci si mohl objednat kdokoliv a ruský botnet k tomu pouze využít. DDoS je relativně běžným nástrojem k páčání hospodářské kriminality.

K aktuálnímu DDoS útoku se však zatím nikdo nepřihlásil. Vyloučit tak lze například zapojení některé ze skupiny Anonymous. Ta totiž v minulosti útoky oznamovala s velkým předstihem a těmi úspěšnými se okamžitě chlubila.

Útok DDoS využívá určité automatické laskavosti a úslužnosti každého webového serveru. Webový server zkrátka "neumí říci ne", když jej někdo požádá o informace, odezvu nebo soubor. V normální situaci je takové chování žádoucí a vede k nejrychlejšímu vyřízení velkého množství požadavků. Každý požadavek je vyřizován v tom pořadí, ve kterém na server dorazil. Pokud ale útočník nebo skupina útočnicků zahltní server falešnými požadavky, může se stát, že server bude na legitimní požadavky reagovat s velkým zpožděním, nebo dokonce vůbec (např. proto, že vyprší časová lhůta pro odpověď).

Tento princip není dobrovolným rozhodnutím provozovatele, ale je daný způsobem fungování síťového komunikačního protokolu TCP/IP. A při útocích se hojně využívá. Mezi nejpoužívanější útoky tohoto typu patří útok distribuovaný (DDoS útok - Distributed Denial of Service Attack). Využívá koordinace desítek, stovek nebo i tisíců počítačů k zaslání falešných požadavků na určitý server s cílem jeho vyřazení. Útočníci se mohou koordinovat pomocí diskusních fór nebo mohou ovládat botnet síť, tedy velké množství virem napadených "zombie" počítačů, ze kterých mohou požadavky vysílat, což ztěžuje jejich vypátrání.

DDoS jsou oblíbenou zbraní v arzenálu aktivistických hackerských skupin, například skupiny Anonymous. Zapojení se do DDoS útoku může být velmi jednoduché. V roce 2010 se např. do DDoS útoků proti bankovním institucím přidala řada fanoušků WikiLeaks.

Obrana před DDoS útoky je často komplikovaná. Kombinuje pasivní a aktivní prvky. Mezi pasivní lze počítat výrazné předimenzování datové propustnosti i schopnosti serveru reagovat na požadavky (i ty falešné). V případě, že si administrátor všimne probíhajícího útoku, může využít i některých nástrojů na aktivní boj s falešnými požadavky.

Druhý den útoků čelil potížím největší český vyhledávač Seznam.cz, jemuž nefungovala hlavní stránka, e-mail a další služby. Provoz byl obnoven asi po třech hodinách od začátku útoku. Jednalo se o cílený útok právě na tento server. Jiné portály ani zpravodajské servery postiženy nebyly.

Identita útočnicků není jasná. V případě iDNES.cz byla většina "falešných" přístupů z Ruska. Server iHNED uváděl, že šlo hlavně o české IP adresy. Vzhledem k tomu, že útočníci IP adresy podvrhovali, není možné z těchto údajů usuzovat na viníky.

Třetí den útoků byl zaměřen na banky a finanční instituce. Mnoha českým bankám nefungovaly webové stránky a především internetové bankovníctví. Bližší informace o jednotlivých případech byly uvedeny v předešlé kapitole věnující se bezpečnosti finančních institucí. Také při tomto útoku se útočníci soustředili na tradiční a velké firmy v daném oboru. Žádné potíže tak neměly servery menších bank, například mBank či AirBank.

Čtvrtý den útoků zacílili hackeři na mobilní operátory. Nefungovaly weby mobilních operátorů O2 a T-Mobile. Naopak Vodafone nebo třeba UPC zvládli útok bez problémů. Útok měl stejně jako u portálu Seznam.cz trvání v řádech několika hodin a stránky obou mobilních operátorů se podařilo ještě téhož dne zprovoznit.

Přehled útoků na českém internetu v posledních letech

- 30. září 2008 - DDos útok, při kterém byly servery zahlceny velkým množstvím dotazů a nefungovaly, postihl zpravodajské weby Blesk.cz a DenikSport.cz, které patří vydavatelství Ringier.
- 29. května 2011 - Hacker napadl den před zahájením písemné části státních maturit internetové stránky s ukázkovými testy a informacemi o zkoušce. Nefungovaly ani stránky organizace Cermat, která maturity zajišťuje. Útočníci nahráli na web vlastní obsah.
- Leden a únor 2012 - Během schvalování kontroverzní dohody proti padělatelství ACTA napadli lidé, hlásící se k hnutí Anonymous, celou řadu českých webů. Terčem útoku byly internetové stránky autorských organizací (Ochranného svazu autorského, Mezinárodní federace hudebního průmyslu IFPI či Intergramu), ale i web ODS nebo stránky Poslanecké sněmovny a vlády. Intenzita a druh útoků byly různé, vedle zahlcení serverů se hackerů podařilo například získat osobní data tisíců členů ODS.
- 14. října 2012 - Internetovou stránku brněnských komunistů napadli hackeři z hnutí Anonymous. Téměř na den na ně umístili nápis, podle něhož jsou voliči KSČM 'omezení idioti'. Web pozměnili po krajských volbách, a to v reakci na úspěch komunistů, jehož v nich dosáhli.
- 16. listopadu 2012 - Hackeři získali databázi z webu exekutorské komory a data umístili na internetu. Skupina Czechurity na svém webu uvedla, že zabavili databázi, neboť exekutoři zabavují majetek občanům. Web komory byl na krátkou dobu po oznámení útoku mimo provoz.

Zdroj: ČTK, idnes.cz, govcert.cz, nbu.cz

Vybrané události ve sledovaném období

Leden

Čína zpřísňuje cenzuru. Na internetu musí být všichni pod svým jménem

Uživatelé internetu v Číně dnes využívají alespoň částečnou anonymitu k blogování, kampaním nebo upozornění na korupci ve státní správě. Nově by však měli všichni na čínském internetu stále vystupovat pod reálným jménem. Nový čínský šéf dohledu nad přístupem k internetu opatření zdůvodnil jako nutná a bezpečnostní.

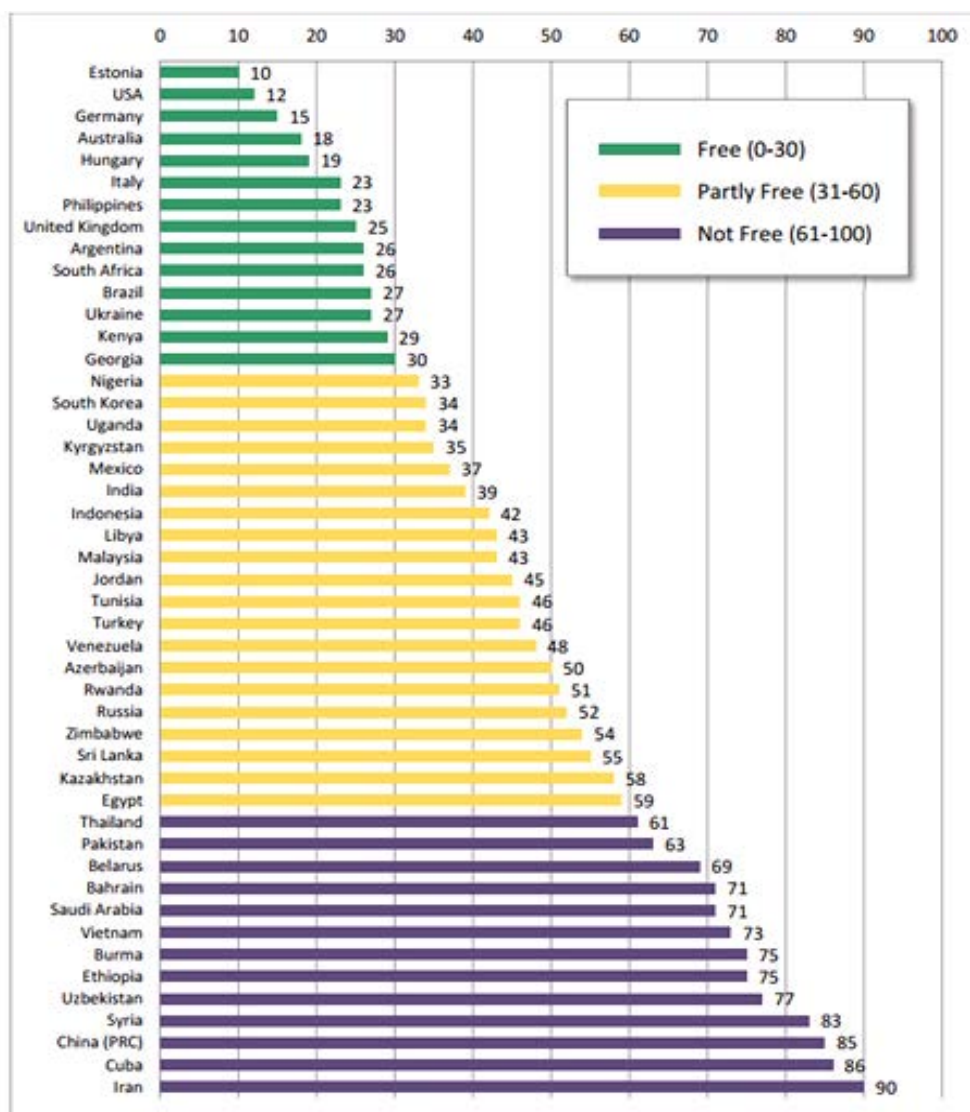
Nově musejí všichni uživatelé internetu všude na webu vystupovat pod svým skutečným jménem. Technické zajištění by se mělo opřít o prohloubenou spolupráci s poskytovateli internetu, mobilními operátory a dalšími provozovateli. Nejde samozřejmě jen o jméno, ale o "úplnou a pravou identifikaci", která umožňuje dohledat on-line příspěvky ke konkrétnímu čínskému občanovi.

Změny jsou podle oficiálního vyjádření navrženy tak, aby "zajistily informační bezpečnost na internetu, zajistily zákonná práva a zájmy občanů a chránily národní zájmy a veřejný sociální prospěch," uvedla čínská státní tisková agentura.

Spekuluje se o tom, že nové nařízení má být reakcí na nedávné případy, kdy anonymní zprávy na internetu pomohly v Číně odhalit korupce na některých místech státní správy. Stalo se tak i na čínských sociálních sítích nebo mikroblogovacích službách (ekvivalenty např. Facebooku a Twitteru).

Čínská vláda podle očekávání tvrdí, že "vítá odhalení a zviditelnění případů, kdy někdo zneužívá svoji autoritu". Korespondent BBC Charles Scanlon se však domnívá, že dosavadní čínská kontrola internetu není již dostatečně přísná. "Nová generace blogerů a komentátorů na čínském internetu představuje hrozbu, se kterou je nové komunistické vedení odhodlané se vypořádat."

Mapa internetové svobody



Přehled internetové svobody. Vyšší hodnota značí vyšší cenzuru. Nejlépe je na tom podle FreedomHouse.org se svobodou Estonsko a USA, nejhůře pak Čína, Kuba a Irán. ČR v žebříčku v důsledku absence dat není zahrnuta.

EU posílí boj s kyberkriminalitou, otevře specializované centrum

Evropská unie chce posílit boj proti nezákonnému zneužívání počítačové techniky. V Haagu začne působit Evropské centrum pro boj proti kybernetické kriminalitě. Jeho cílem bude chránit proti této formě zločinné činnosti evropské firmy a občany.

'Centrum pro boj proti kybernetické kriminalitě velmi napomůže evropskému boji proti tomuto druhu zločinnosti a přispěje k tomu, abychom měli svobodný, otevřený a bezpečný internet,' prohlásila k zahájení činnosti centra eurokomisařka pro vnitřní záležitosti Cecilia Malmströmová. 'Pachatelé tohoto typu trestné činnosti jsou velmi chytří a rychle si osvojují nové technologie, aby je zneužili k nezákonné činnosti,' dodala.

Středisko bude sídlit v Haagu v rámci Evropského policejního úřadu (Europol). Šéf vznikajícího střediska Troels Oerting zdůraznil, že je třeba vzít v úvahu, že počítačovou kriminalitu neomezují žádné hranice a pachatele je těžké vypátrat.

Centrum by tak mělo pomoci shromažďovat údaje z různých zemí, analyzovat je a podporovat vyšetřování v jednotlivých zemích. Poskytovat by také mělo odborné poradenství během soudních řízení. Zaměří se i na nezákonnou činnost páchanou skupinami organizovaného

zločinu prostřednictvím internetu, zejména na útoky na elektronické bankovníctví, i další finanční aktivity prováděné na internetu. Zapojit by se mělo i do výzkumu a vývoje nových nástrojů, které je možné v boji s touto kriminalitou používat.

Komise dnes také podotkla, že na světě každý den se stane obětí nějakého druhu kybernetické kriminality zhruba milion lidí. Odhady pak hovoří o tom, že oběti kvůli této činnosti přijdou ročně na světě o 290 miliard eur.

Únor

Vládní instituce v různých zemích ohrožuje nový virus MiniDuke

Významné vládní instituce více než dvaceti zemí, včetně České republiky, byly v minulém týdnu napadeny novým nebezpečným počítačovým virem označovaným MiniDuke. Virus útočí prostřednictvím infikovaných souborů v hojně užívaném formátu PDF a podle ruské bezpečnostní firmy Kaspersky Lab z vládních počítačů získává 'geopolitické informace'. Terčem útoku se stala i Severoatlantická aliance.

Virus MiniDuke podle odborníků zaútočil na vládní systémy na Ukrajině, v Belgii, Portugalsku, Rumunsku, v České republice a v Irsku. Kromě toho napadl i některé výzkumné či zdravotnické instituce ve Spojených státech a v Maďarsku. Česká policie informace o hrozbě zná, závažné problémy ale údajně nenastaly, sdělila ČTK mluvčí policejního prezidia Štěpánka Zatloukalová. Útok neznámých hackerů pocítila i Severoatlantická aliance, i když její počítačové systémy údajně neutrpěly žádné škody. Centrála NATO nicméně v prohlášení uvedla, že zachovává ostražitost a o útoku informovala členské státy.

Hackeri postavili svou novou zbraň na bezpečnostních mezerách, které objevili v softwarových nástrojích firmy Adobe, mimo jiné v jejím programu ke zobrazování dokumentů ve formátu PDF. Obětem rozesílají na první pohled nevinné soubory v tomto formátu nakažené virem. Dokumenty obsahují smyšlený, ale kvalitně zpracovaný text týkající se kupříkladu semináře o lidských právech, zahraniční politiky Ukrajiny nebo plánů této země na členství v NATO. Virus pak ve vládních počítačích vyhledává utajované informace, které jsou podle firmy Kaspersky 'geopolitické povahy'. Podle maďarského výzkumného týmu CrySyS napadl virus už desítky organizací, ale hlavní cíl jeho útoku zůstává jen předmětem spekulací. Odborníci si ani nejsou jisti, jak daleko útok na vládní servery pokročil. Neví se například, zda virus už začal získané údaje vyhodnocovat a odesílat zpět původcům útoku. Žádné informace nejsou ani o identitě útočníků kromě toho, že hlavní servery mají v Turecku a Panamě. Na rozdíl od známých špionážních virů Stuxnet a Flame, které se podle všeobecného mínění zrodily v amerických nebo izraelských státních laboratořích, stojí zřejmě za novým virem zločinecké podsvětí. Komplikovanou stavbou a zákeřností se MiniDuke řadí mezi nejnebezpečnější produkty hackerů.

Hackeri napadli Twitter, mohli získat až čtvrt milionu hesel

Získání informací ze čtvrt milionu uživatelských účtů je jeden z největších bezpečnostních skandálů, jakým Twitter od svého vzniku čelil. Sociální síť Twitter využívá po celém světě zhruba 200 milionů lidí a poškozené uživatele o možném úniku jejich přihlašovacích údajů okamžitě informovala. Hackerský útok přišel poté, co Twitter varoval uživatele, že se někdo pokouší získat přístup k jejich datům. Jeden z útoků se jim podařilo detekovat.

Bezpečnostní experti varovali, že hackeri teď mají v rukou cenné informace. Uživatelé často používají stejná hesla i uživatelská jména také pro jiné účely, například internetové bankovníctví. Experti ze sociální sítě se domnívají, že neútočili amatéři a nešlo ani o ojedinělý případ. "Útočníci byli velmi důmyslní, obáváme se, že podobný útok čeká brzy i další společnosti," uvedl Twitter s tím, že v hledání pachatelů spolupracují s americkou policií i s vládou.

Jeden z expertů se domnívá, že hackeri sociální síť napadli nejspíše přes počítač někoho ze zaměstnanců. Za poslední dobu čelilo útoku hackerů více internetových serverů. Deníky The New York Times a Wall Street Journal informovaly o napadení hackery z Číny. Čínské velvyslanectví ve Washingtonu i úřady v Pekingu se zdržely vyjádření, od útoků se však distancovalo čínské ministerstvo obrany.

Hackeri napadli Facebook, data uživatelů nebyla ohrožena

Několik týdnů prý Facebook čelil útoku hackerů. Ti zneužili chybu v systému Java, aby úspěšně napadli několik počítačů zaměstnanců firmy a dostali se do nich. Podle prohlášení firmy nebyla ohrožena data uživatelů.

Facebook oficiálně oznámil, že zjistil, že některé počítače patřící inženýrům Googlu byly hacknuty pomocí tzv. zero-day chyby v programu Java. Nezabezpečený problém v jednom z hojně rozšířených systémů pro práci s multimediálním obsahem na internetu umožnil útočnickům proniknout do počítačů napadených a nainstalovat tam škodlivý software (malware).

Firma oznámila, že nenašla žádné důkazy, které by prokázaly, že došlo k úniku osobních dat. Facebook aktuálně využívá více než miliarda lidí po celém světě.

Podle serveru Ars Technika, bylo napadeno jen několik notebooků. Útok byl objeven, když byla objevena podezřelá doména ve facebookových záznamech. Tyto žádosti byly sledovány zpět k notebooku inženýra pracujícího na vývoji projektu mobilní aplikace. Forenzní analýza souborů na notebooku vedla k objevu řady dalších napadených systémů.

Útočníci přitom patrně nepoužili oblíbený scénář, kdy navedou uživatele pomocí e-mailu či odkazu na upravenou stránku, která jim umožní napadnout počítač. Tentokrát se jim podařilo vložit závadný kód přímo do regulérního webu, který byl určen pro vývojáře mobilních aplikací.

Microsoft a Symantec překazily obří útok, odpojily statisíce počítačů

Podle agentury Reuters, která zprávu o překaženém útoku přinesla, bylo bez vědomí uživatelů nakaženo 300 až 600 tisíc počítačů. Podle Symantecu je nakažených počítačů více než milion. Malware (škodlivý software) neboli botnet nazvaný Bomital spojil napadené počítače do obří sítě, ve které mohly být centrálně ovládány a zneužity pro útoky na vybrané stránky, rozesílání spamu atd.

Primární důvod útoku však byl jiný. Útočníci přesměrovali výsledky vyhledávání služeb Google, Yahoo a Bing na podvržené spřízněné stránky. Vydělávali tak na on-line reklamě, kdy zadavatel reklamy platí za každý proklik uživatele (zákazníka) na daný odkaz (reklamu). V angličtině má tento podvod příznačný název click fraud.

Jakmile Microsoft a Symantec útok odhalily, byli majitelé nakažených počítačů při pokusu o připojení na web přesměrováni na speciální stránku, obdrželi od jmenovaných firem varovnou zprávu a link na nástroj ke smazání viru. V textu zprávy je mimo jiné uvedeno, že ji budou dostávat do té doby, dokud škodlivý software z počítače neodstraní.

Navrhovaný EU zákon o kybernetické bezpečnosti upevní povinnost aktivně reportovat

Nová pravidla EU týkající se kybernetické bezpečnosti byla prezentována po řadě týdnů spekulací a dílčích úniků informací. Nejdůležitější část Strategie kybernetické bezpečnosti Evropské komise se jmenuje nařízení síťové a informační bezpečnosti (Directive on Network and Information Security). V případě, že bude strategie přijatá Evropským parlamentem a členskými státy, stane se součástí práva EU.

Putin rozhodl o vzniku protihackerské obrany

Ruský prezident Vladimir Putin rozhodl o vzniku ruského obranného systému proti hackerským útokům pod hlavičkou FSB (Federální služba bezpečnosti - ruská kontrarozvědka i zpravodajská služba vnitřní bezpečnosti). Podnětem bylo s velkou pravděpodobností odhalení kauzy "Red October" antivirovou společností Kaspersky Lab. "Red October" označuje malware, který je zaměřen na získávání diplomatických a vědeckých informací z Ruska a postsovětských zemí. Tyto informace byly často klasifikované (utajované) a obsahovaly i velmi citlivé údaje o výzkumu a vývoji moderních zbraňových systémů. Kauze „Red October“ byl blíže věnován prostor v minulé Situační zprávě o vybraných sektorech bezpečnosti.

Obama vydal nařízení k obraně proti kybernetickým útokům

Americký prezident Barack Obama vydal nařízení zaměřené na zlepšení obrany před kybernetickými útoky. Učinil tak v poselství o stavu unie. Důležité americké podniky podle nařízení mají sdílet informace o akcích ohrožujících jejich

kybernetickou bezpečnost, jimiž jsou zejména útoky hackerů. Tajné služby zase dostaly za úkol analyzovat rizika hrozící těmto firmám například z oblasti infrastruktury či bankovníctví, a více než dnes poskytovat informace o případných kyberútocích, které těmto společnostem hrozí.

Jde o zatím nekomplexnější plán, kterým se Obama chce postavit proti elektronickým útokům na amerických počítačových sítích. Opatření představuje novou snahu o zpevnění elektronického obranného valu po loňském masivním náporu zejména v oboru průmyslové špionáže, ze kterého odborníci obviňují především Čínu.

Součástí nařízení je i vytvoření nového rámce a pravidel pro kybernetickou bezpečnost. Tímto úkolem pověřil Obama Národní institut pro standardy a technologie (NIST), který bude na vytvoření těchto základů spolupracovat s vlastníky firem.

Obama vydal příslušné nařízení poté, co loni neprošel v Kongresu navrhovaný zákon o ochraně před kybernetickými útoky.

Březen

České weby čelily největšímu útoku v historii

Nejprve byly napadeny servery iDNES.cz, iHNED.cz, Novinky.cz, Lidovky.cz a deník.cz. Menší vlna zasáhla i jiné weby, které však zaznamenaly pouze lehké problémy. Téhož dne podlely útokům také servery Živě.cz, Mobilmania.cz nebo E15. Ochromen byl druhý den útoků i největší český vyhledávač Seznam.cz. Třetí den útoků se hackeři zaměřili na banky (ČSOB, Komerční banka, Českou spořitelnu, Raiffeisenbank a UniCredit Bank). Čtvrtý den útoků byly ochromeny weby mobilních operátorů O2 a T-Mobile. Hackeři tedy primárně útočili na velké firmy ve svých oborech.



Tajné služby údajně umí odposlouchávat Skype: hovory i textové zprávy

Ruský deník Vedomosti uvedl, že ruské tajné služby jsou schopné odposlouchávat konverzace přenášené programem Skype. Program je totiž možné přepnout do speciálního režimu, ve kterém jsou šifrovací klíče generovány serverem, nikoli počítačem či telefonem, na kterém Skype běží. Díky tomu je teoreticky možné konverzaci rozšifrovat.

V Číně jsou zase uživatelé, kteří si chtějí stáhnout program Skype z adresy skype.com, přesměrování na server skupiny TOM Online. Uživatelé si zde stáhnou alternativní verzi programu Skype (dále TOM-Skype), která umožňuje komunikaci podobně jako běžný Skype a rovněž nese klasické modré logo Skype. Program však sleduje určitá slova, jejichž seznam je zašifrovaný, a o těch pak informuje centrální server.

Potápěči chtěli odříznout Egypt od internetu

Obyčejná rybářská loď byla základnou potápěčů, které egyptská pobřežní hlídka přistihla při poškozování podmořských kabelů. Pokud by se jim podařilo kabely přerušit, severoafrická země by přišla o polovinu své internetové konektivity.

Internet zahlcen útokem zhrzených spamerů

Tento útok je prý odvetou za zablokování holandské skupiny CyberBunker, kterou nezávislá skupina Spamhaus přidala na spamovou černou listinu.

CyberBunker po zásahu Spamhausu uvedl, že organizace zneužívá svou pozici k rozhodování o tom, co může a nemůže být na internetu. Sám prosazuje politiku hostingu všeho kromě dětské pornografie a materiálů spojených s terorismem.

Útočníci používají hrubou taktiku v podobě DDoS útoků, které velkým množstvím zasílaných dotazů zahltní napadený web a snaží se jej vyřadit z provozu. Cílem útoků jsou primárně servery

Spamhausu, ale vzhledem k jejich napojení na Systém doménových názvů (DNS) by mohly zahltit internetovou infrastrukturu.

Duben

Systém předvídání živelných katastrof Copernicus bude sídlit v Praze

Po centrále navigačního systému Galileo se v Česku patrně objeví další vesmírný projekt Evropské unie. Je jím systém Copernicus, který bude mít na starosti sledování Země. Projekt Copernicus je známější pod původní zkratkou GMES (Global Monitoring for Environment and Security - globální monitoring životního prostředí a bezpečnosti). S využitím informací ze satelitů a pozemských měřicích stanic předpovídá možné živelné katastrofy a pozoruje změny klimatu.

Takový monitoring například umožňuje dřívější zásah při přírodních katastrofách, což by mělo snižovat ztráty na životech i majetku. Díky monitoringu i meteorologickým předpovědím by se také měly optimalizovat zemědělská produkce, rybolov, turistický ruch, doprava nebo třeba urbanistický rozvoj. Centrála projektu Copernicus by se měla přesunout do Prahy, do stejné budovy, kde již nyní sídlí centrála projektu Galileo.



Když vypukne kyberválka, bude se střílet i do civilistů

Civilní kyberútočník se může stát vojenským cílem. Pokud ohrozil majetek či životy, nevztahuje se na něj ochrana civilistů. Shodli se na tom po třech letech experti na mezinárodní právo NATO.



Příručka "Tallinský manuál" radí, jak právně řešit válku v kyberprostoru. Do značné míry vychází z otázek, které se řešily už kvůli atomové bombě.

Kyberválka, tedy válka vedená prostřednictvím počítačových sítí, už dávno nepatří jen do sci-fi. Spojené státy i NATO se na ni pečlivě připravují, a to jak prakticky, tak i teoreticky. Nejnovějším příspěvkem do kontroverzní debaty o tom, co je v takovém novodobém konfliktu dovoleno, je tzv. Tallinský manuál. Spolu s názorem zástupce amerického Ministerstva obrany na válku kyberprostoru jde o nejvýznamnější dokument mapující pohled

mezinárodního práva na nový typ války.

Experti se shodli, že "to, že je útok vedený počítačově, nemá vliv na to, zda je na něj nahlíženo jako na použití síly". S přesnou definicí ovšem byly trochu problémy. Jako "použití síly" ve vojenském slova smyslu je kyberútok považovaný ve chvíli, kdy způsobil ztráty na životech či zdraví, či významné poškození fyzických objektů či infrastruktury. Za "použití síly" by zřejmě nebylo považováno samotné smazání či odcizení dat, pokud by neměly za následek něco z výše uvedeného.

Stát tedy může v kyberválce útočit na počítačové systémy, které jsou označeny jako vojenské cíle. Pokud jde např. o počítačovou síť, která slouží pro civilní i armádní účely, lze ji podle většiny odborníků považovat za cíl vojenský. Jistou výjimku by v tomto případě mohly podle některých zúčastněných představovat např. sociální sítě - i kdyby je armáda využívala k šíření svých zpráv, neospravedlňuje to útok na jejich servery, protože zde není dodržena podmínka adekvátní reakce.

Manuál zdůrazňuje ochranu civilistů před kyberútoky. Je ale dobré zdůraznit, že útokem se zde rozumí naplněná podmínka zmíněná výše, a sice "škoda na životě, zdraví či fyzická újma na majetku" v důsledku útoku (ať již počítačového, kybernetického, či klasického, kinetického). Zatímco tedy cizí stát nesmí na dálku napadnout např. auto civilisty a tím jej ohrozit, může zřejmě

napíchnout jeho počítač, odposlouchávat či vést psychologickou válku (tzv. PSYOP). Stejně tak nemusí stát zvažovat, zda útokem na vojenské cíle nezpůsobí civilistům nepohodlí či stres. To vše se ovšem týká civilistů, kteří se nepřidali k armádě, ozbrojenému odporu nebo útočící skupině. Hacker, ač civilista, se vzdává práva na ochranu před vojenským útokem nepřátelské strany, pokud se do bojů aktivně zapojí.

Jako zapojení do útoku se přitom počítá i např. DDoS útok vedený proti klíčovým vojenským sítím. Netýká se to naopak programátora, který vyvine software umožňující napadení nepřátelských sítí - teprve použití takového software dává armádě právo na takového programátora zaútočit.

Zvláště ošemetnou otázkou je tzv. preventivní útok, tedy snaha předejít kyberútoku vlastním útokem. Experti, kteří se podíleli na Tallinském manuálu, se shodují, že stát se může kyberútokům bránit ve chvíli, kdy je jisté, že cizí stát jej chce napadnout. Případně alespoň že skupina, která jej chce napadnout, je podporovaná jistým státem. USA se rozchází s panelem expertů v tom, zda je povolený zásah proti cílům, které nejsou vojenské, ale pomáhají "udržovat válku", tedy například ropné rafinérie či elektrárny. Menší shoda také panuje o tom, jak je to se skupinou (např. teroristů), která není přímo podporovaná konkrétním státem.

Květen

Podvodné e-maily obsahující virus

Podvodné e-maily, které se tváří jako zprávy od mobilních operátorů, začaly chodit i z adresy noreply@o2.com, která vypadá jako od Telefoniky. Zpráva s přílohou vydávající se za MMS obrázek obsahuje nový vir, který stávající antivirové programy nedokážou rozpoznat. Na svých stránkách o tom informoval Národní tým pro koordinaci řešení bezpečnostních incidentů v počítačových sítích CSIRT.

Virus v příloze slouží ke stahování dalších škodlivých programů z předem definovaných webových adres. Po jejich stažení se může uživatelův počítač stát například součástí sítě ovládaných počítačů nebo se díky tomuto viru mohou útočníci dostat k osobním údajům. Může tedy dojít k ohrožení přihlašovacích údajů uživatelů, včetně přihlašovacích údajů k internetovému bankovníctví.

Počty adresátů podvodných e-mailů jsou podle bezpečnostního analytika CSIRT.CZ Pavla Bašty řádově minimálně tisíce. 'Je potřeba si uvědomit, že vzhledem k existenci antivirových řešení na úrovni mail serverů, vzhledem k existenci antivirů na počítačích uživatelů a také díky osvětě a lepší informovanosti uživatelů bude procento reálně infikovaných počítačů poměrně malé, proto útočníci musí svou zprávu zaslat co nejvíce obětem,' uvedl.

Nedávno se objevily podobné zprávy posílané jménem T-Mobilu a minulý měsíc i od Vodafonu. Obdobný útok zaznamenal nedávno i Skype.

Červen

USA přiznaly „šmírování“

Informaci přinesly The Washington Post a The Guardian na základě tipu od utajeného zdroje přímo z NSA. Údajné sledování a analýza komunikace mají probíhat prostřednictvím přístupu specializovaných agentů přímo na servery kooperujících firem. Kromě NSA, která spadá pod ministerstvo vnitra, má k datům z operace PRISM přístup zřejmě i FBI, příslušející ministerstvu spravedlnosti.

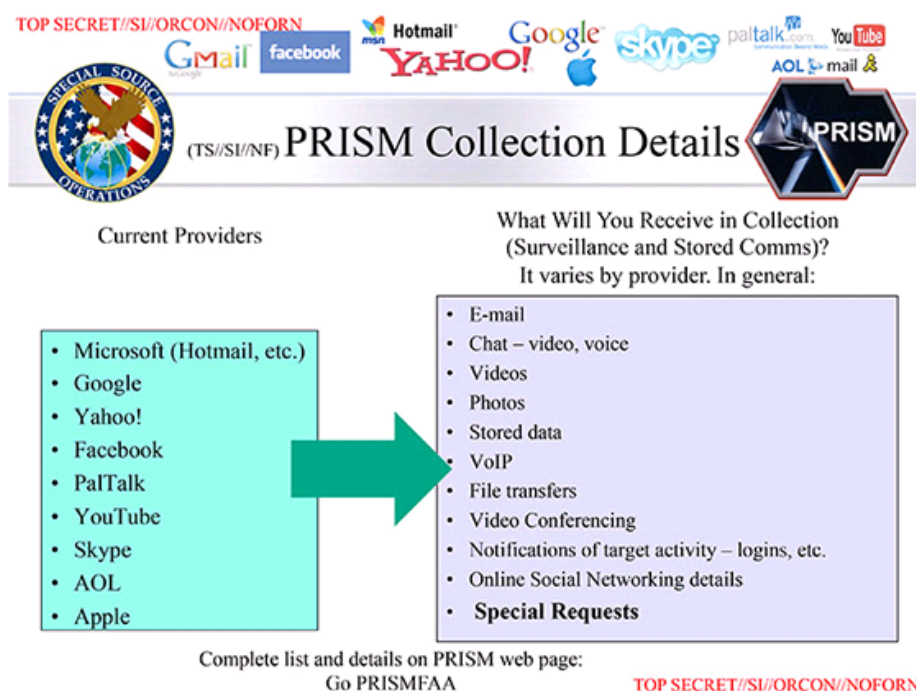
Sledování probíhá kombinací strojové analýzy a následného procházení dat konkrétními odborníky NSA. Hlavním deklarovaným cílem je odhalování mezinárodních hrozeb, zločinu a terorismu. Je to právě možnost strojového přístupu přímo k datům na serverech, která znepokojuje odbornou veřejnost nejvíce. Dosud se vědělo pouze o přístupech na vyžádání, na základě např.



soudního příkazu.

Prezentace o operaci PRISM, kterou vynesl z NSA utajený zdroj, je určena pro výše postavené analyticky na ředitelství NSA. Vychvaluje její účinnost. Jen loni se z ní čerpalo ve zprávách pro prezidenta 1 477krát a čerpá se z ní asi sedmina dat rozvědky. Přístup k datům je prakticky okamžitý, protože není potřeba čekat na soudní příkaz či podobné rozhodnutí. NSA si může ze serverů spolupracujících firem vytáhnout cokoli, ovšem podle pravidel by si neměla ukládat všechna data, ale postupovat selektivně.

Agenti mohou díky datům z operace PRISM získat například e-maily, fotografie, videa, soubory, videokonference, výpis aktivit, zprávy ze sociálních sítí a soukromé zprávy (chat). Jediným omezením při přístupu k datům je nařízení, aby takto nebyli sledováni američtí občané. Jako první se ke spolupráci přidal Microsoft, v roce 2007. Google a Facebook se připojili v roce 2009, poslední se přidal Apple v roce 2012.



Britové „šmírují“ víc než USA

Zastaralý zákon zřejmě umožňuje Velké Británii ještě rozsáhlejší „šmírování“, než jaké provádí americké tajné služby. Monitorují data proudící optickými kabely: telefony, e-maily i další internetovou komunikaci. Podle Edwarda Snowdena zde není téměř žádná kontrola a vše je dovoleno. Lidé z britské GCHQ oponují: sledují prý jen podezřelé "jehly v kupce sena".

Napíchnutí optických kabelů provedla britská tajná služba ve spolupráci s tzv. odposlouchávacími partnery. Jsou jimi velké firmy, jejichž identita je skrytá dokonce i v rámci interní prezentace - prý kvůli případnému politickému skandálu. Tyto firmy mají nakázanu mlčenlivost o tomto programu a své zapojení musejí popřít.

Sondy jsou umístěny na optické kabely pravděpodobně v místech, kde vstupují na území Velké Británie. Po těchto linkách ovšem vzhledem k podstatě internetových protokolů probíhá často i komunikace vnitrostátní. Celkově je napíchnuto asi 200 kabelů, současně vybavení umožňuje GCHQ ukládat data ze 46 z nich zároveň.

KRIZOVÉ ŘÍZENÍ

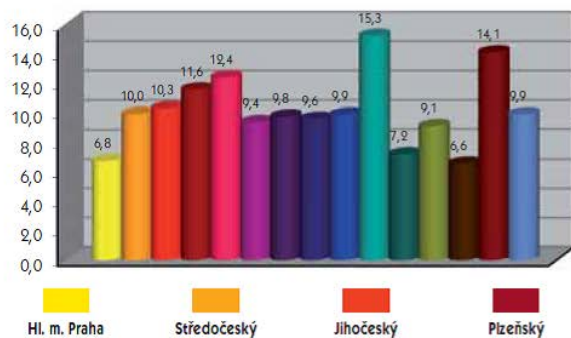
Statistiky a jejich interpretace

Namísto policejních statistik se v tomto případě soustředíme na statistiky Generálního ředitelství Hasičského záchranného sboru ČR, konkrétně na data z období 1.1. – 31.3. 2013 a částečně na souhrnná data za rok 2012. Tyto statistické výstupy jsou v podrobnější verzi pravidelně aktualizovány rovněž na stránkách www.hzscr.cz. Data za druhé čtvrtletí jsou dosud zpracovávána.

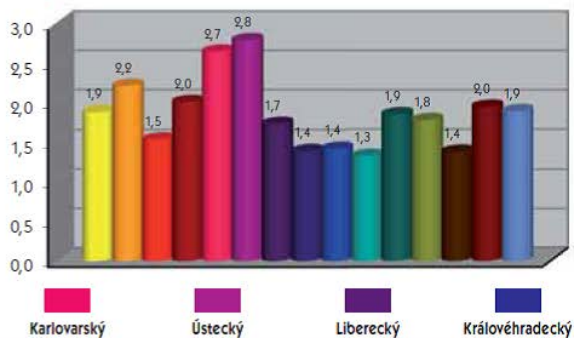
V období od 1. ledna do 31. prosince 2012 zasahovaly jednotky požární ochrany u 103 985 událostí, což je o 2 884 událostí více než za rok 2011. Nejčetnějšími událostmi byly technické havárie – 50,1 %, následují požáry – 19,1 %, dopravní nehody – 18,2 %, úniky nebezpečných chemických látek – 4,9 %. Události podle krajů jsou znázorněny na následujících grafech.

Události podle krajů (počet na 1 000 obyvatel)

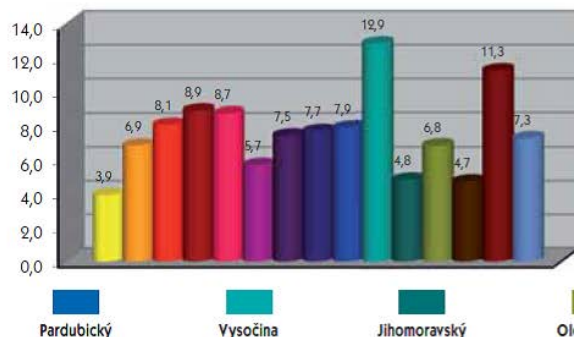
Události celkem



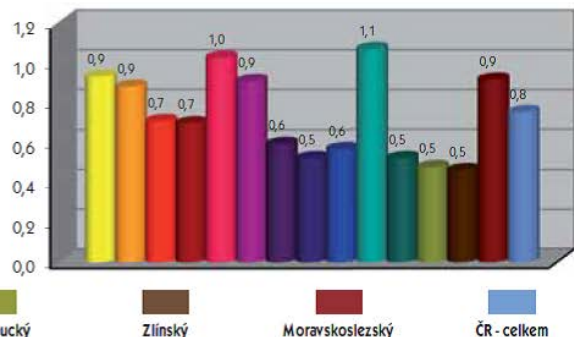
Požáry



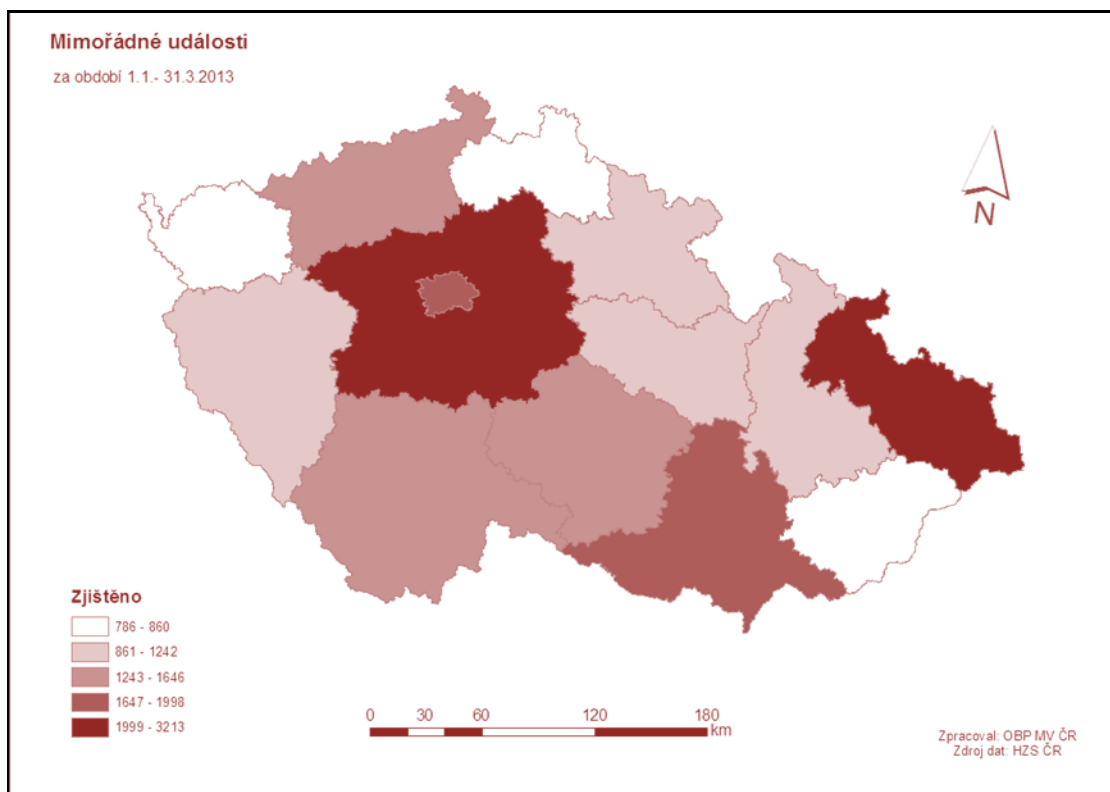
Technické zásahy



Plané poplachy



Rozložení mimořádných událostí za první čtvrtletí roku 2013 podle jednotlivých krajů znázorňuje následující mapa.



V prvním čtvrtletí roku 2013 zasahovaly jednotky PO u 21 529 událostí, což je o 12% méně než ve stejném období roku 2012. Nejčtenějšími událostmi byly technické havárie – 50,1%, dopravní nehody – 21,5%, požáry – 16,9%, úniky chemických látek – 4,3%. Plané poplachy tvoří 7% z celkového počtu událostí.

Počet **požárů** poklesl o 40 %. Na příznivý vývoj měl vliv především nižší počet požárů volných skládek, odpadů, lesních porostů a požárů v přírodním prostředí vůbec, vlivem vlhkého a chladného počasí na celém území ČR.

Počet **dopravních nehod** likvidovaných jednotkami PO oproti loňskému roku vzrostl o 8 %. Nejčtenější byly zásahy u dopravních nehod v hl. m. Praze – 147 (-30) a v okr. Ústí nad Orlicí – 140 (+18), minimum v okrese Teplice – 23 (+1). Celkově u dopravních nehod hasiči bezprostředně zachránili 1 461 osob (+601), při zásazích se vyskytlo 137 (+14) usmrcených osob a také 2 809 (+225) zraněných osob, jimž v mnoha případech poskytli předlékařskou pomoc.

Při **únicích nebezpečných chemických látek** jsou v prvním čtvrtletí letošního roku nejčtenější úniky ropných produktů – 668 (-136), úniky plynů včetně aerosolů – 175 (-16), dále úniky kapalin mimo ropných produktů – 60 (0), pevných látek – 0 (-5) a ostatních látek včetně potravinářských produktů – 31 (+15). Nejvyšší počet těchto případů byl v hl. m. Praze – 170 (+3), žádný v okrese Ústí nad Orlicí a Svitavy.

Skupina **technické havárie** zahrnuje technické havárie – 3 (-12), dále technické pomoci – 9 449 (-246), technologické pomoci – 174 (+41) a ostatní pomoci – 1 169 (-62). Jsou doménou jednotek Hasičského záchranného sboru ČR jako pomoci v nouzi při otvírání uzavřených prostorů, odstraňování překážek na komunikacích, vyprošťování osob, zvířat či předmětů apod. Nejvíce případů je evidováno v Ostravě – 958 (-224), v hl. m. Praze – 838 (+67), nejmenší počet v okrese Semily – 32.

Radiační nehoda či havárie nevznikla.

Počet **planých poplachů** se oproti loňskému období snížil o 18 %, přičemž jejich podíl na celkovém počtu událostí se snížil na 7,0 %. Nejčetnější (46 %) jsou plané poplachy způsobené elektrickou požární signalizací, další plané poplachy jsou způsobeny přivoláním k případu, který měl příznak požáru (18 %), přivolání k nenahlášenému pálení (9 %), zneužití jednotky PO (7 %) a jiné důvody (20 %). Nejvíce planých poplachů bylo v hl. m. Praze – 247 (+16), v okrese Kutná Hora je evidován jen 1 planý poplach.

Jednotky PO zachránily či evakovaly z bezprostředně ohrožených prostor, zejména při požárech, dopravních nehodách a technických pomocích, v letošním prvním čtvrtletí **8 848** osob, což je o 533 osob více než za stejné období v roce předchozím. Při zásazích bylo zraněno **74** profesionálních a **19** dobrovolných hasičů.

Při zběžném pohledu se zdá, že počet neštěstí v zásadě odráží počet obyvatel v jednotlivých krajích, bližší zkoumání ale odhalí některé zvláštnosti. Při přepočtu na velikost populace je na tom totiž daleko nejhůř kraj **Vysočina**, který, ač patří mezi oblasti s nejnižší hustotou osídlení, počtem mimořádných událostí převyšuje výrazně lidnatější kraje.

Nejčastěji museli hasiči zasahovat v Moravskoslezském a Středočeském kraji, které patří mezi nejlidnatější v zemi. **Moravskoslezský kraj zaznamenal 3 213 mimořádných událostí, Středočeský 2 678, Jihomoravský kraj pak 1 998. V Praze bylo evidováno 1 854 mimořádných událostí.**

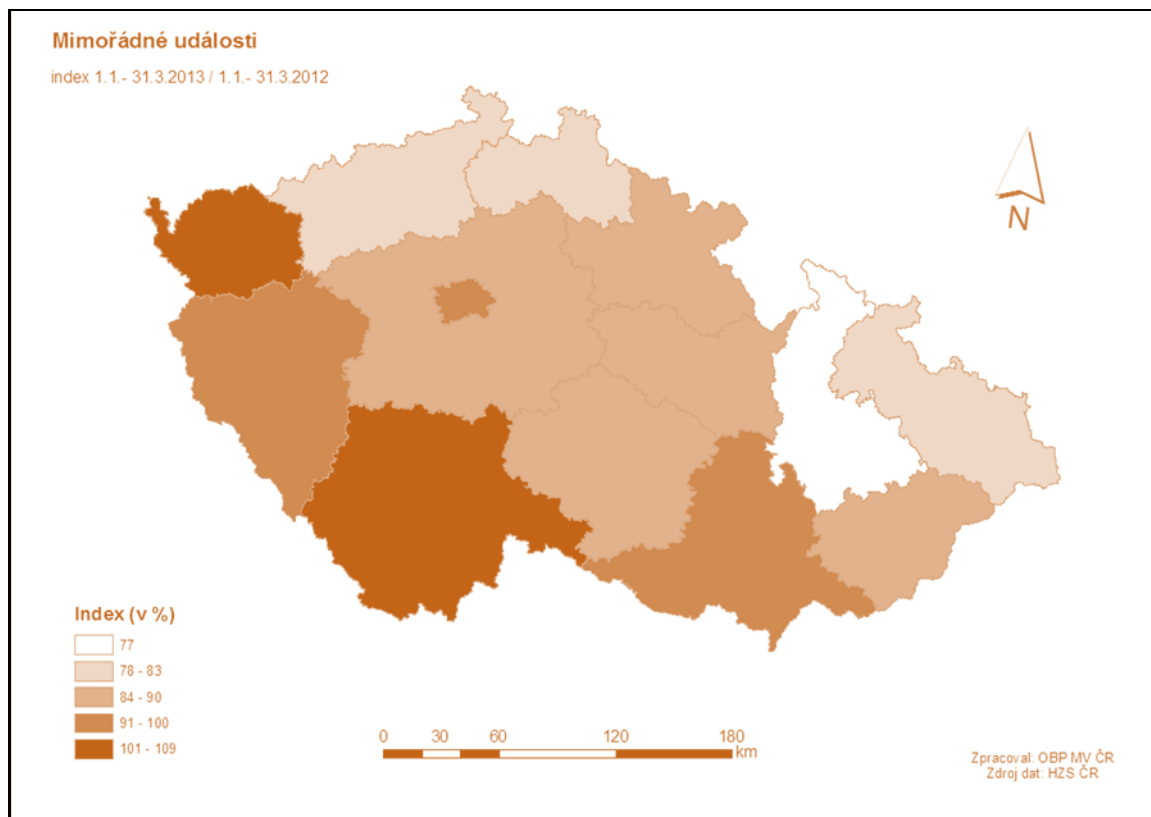
Na druhou stranu byl ovšem v Moravskoslezském kraji zaznamenán pokles počtu mimořádných událostí oproti roku 2012 o 781 událostí, ve Středočeském kraji klesl počet mimořádných událostí o 307, v Jihomoravském kraji o 131, v Praze o 61. Přehled krajů a pokles či nárůst počtu mimořádných událostí v prvních čtvrtletích letošního a loňského roku je patrný z níže uvedené mapky.

Tabulka znázorňující jednotlivé druhy událostí za první čtvrtletí let 2011, 2012 a 2013.

Druh události	2011	2012	2013
Požáry s účastí jednotky PO	5 815	6 081	3 642
Dopravní nehody	3 538	4 292	4 636
Úniky nebezpečných látek	1 135	1 076	934
z toho „ropných produktů“	859	804	668
Technické havárie	9 265	11 074	10 795
Radiační havárie a nehody	0	0	0
Ostatní mimořádné události	4	4	8
Plané poplachy	1 791	1 851	1 514
UDÁLOSTI CELKEM	21 548	24 378	21 529

Zdroj: MV-GŘ HZS ČR

Mapka znázorňující pokles/vzrůst počtu mimořádných událostí za období 1.1.2013 – 31.3.2013 a 1.1.2012 – 31.3.2012.



Členění zásahů u událostí vyvolaných negativním působením přírodních sil a jevů za období leden – březen 2013 je následující:

celkem 1 874 (-186) zásahů, z toho:

12 u požárů (-10) (způsobených zejména bleskem),

428 u dopravních nehod (-175),

5 při úniku nebezpečné chemické látky (+5),

1 420 u technických havárií (-348),

9 u ostatních událostí a planých poplachů (+2).

Nejčastěji hasiči zasahovali v úterý – 16,6%, nejméně událostí se stalo v neděli – 12,8%.

V období od 1. 1. do 31. 3. 2013 vzniklo v ČR **3 798** požárů (s účastí i bez účasti jednotek PO). Přímé škody dosáhly částky **596,8** mil. Kč, **44** osob bylo usmrceno a dalších **351** osob zraněno. Počet požárů je letos oproti stejnému období loňského roku nižší o 39,5%, škody jsou vyšší o 8,4%. Počet usmrcených osob je nižší o 14% a počet zraněných nižší o 10%. Jednotky PO uchránily před zničením hodnoty za **4 570,0** mil. Kč.

Nejvíce požárů vzniklo v hl. m. Praze – 460 (-121) a v okr. Karviná – 130 (-48). Nejméně požárů bylo v okr. Plzeň jih – 13 (-18).

Tabulka znázorňující počet požárů za první čtvrtletí let 2011, 2012 a 2013, včetně škody vyjádřené v milionech Kč a počtu usmrčených a zraněných osob.

Rok	Počet požárů	Škoda mil. Kč	U	Z
2011	6 034	473,0	34	275
2012	6 265	550,5	51	390
2013	3 798	596,8	44	351

Oproti loňskému 1. čtvrtletí vzrostla četnost požárů pouze u vznícení následkem dopravních nehod, u ostatních příčin je pokles.

Požáry beze škody - přírodních porostů, popelnic, kontejnerů a odpadů, demolic a vraků, vznícení potravin při vaření, vznícení sazí v komíně - tj. kategorie požárů dále nedošetřených, tvoří letos 48 % z celkového počtu požárů a zaznamenaly pokles oproti loňskému 1. čtvrtletí, a to o 50 %.

Z celkového počtu **44** usmrčených osob při požárech bylo:

- 3 děti do 15 let,
- 33 osob ve věku od 15 do 60 let,
- 8 osob ve věku nad 60 let.

Tabulka informující o příčinách požárů v prvních čtvrtletích let 2011, 2012 a 2013

Příčina/rok	2011	2012	2013	Index 13/12
Úmyslné zapálení	469	363	312	86
Hra dětí s ohněm	60	49	19	39
Nedbalost dospělých	758	902	537	60
Závady komínů	147	174	149	86
Závady topidel	60	72	56	78
Technické závady (mimo komínů a topidel)	640	691	602	87
Samovznícení	10	16	9	56
Výbuchy	6	7	3	43
Dopravní nehody	20	27	29	107
Dále nedošetřované požáry	3 529	3 642	1 828	50
Ostatní příčiny	7	11	10	91
Neobjasněno, v šetření	328	311	244	78
CELKEM	6 034	6 265	3 798	60

Zdroj: MV-GŘ HZS ČR

Přehled velkých požárů se škodou 10 milionů Kč a vyšší za čtvrté čtvrtletí roku 2012

12. 10. • Sportovní hala SPORT EDEN, o.s., Beroun.

Příčina: elektrický zkrat fotovoltaického panelu.

Škoda: 15 000 000 Kč.

Zraněn: 1 hasič.

14. 10. • Skladová hala, tři nákladní automobily a člun, Roudnice nad

Labem-Podluský, okr. Litoměřice.

Příčina: technická závada – proudové přetížení.

Škoda: 12 300 000 Kč.

31. 10. • Transformátor fotovoltaické elektrárny firmy WIS ENERGO

LEDCE SEVER, spol. s r.o., Ledce, okr. Brno-venkov.

Příčina: nepředpokládané změny provozních parametrů.

Škoda: 11 600 000 Kč.

2. 11. • Hotel KUBA, Kubova Huť, okr. Prachatice.

Příčina: technická závada na ventilu tlakové láhve s propan butanem.

Škoda: 10 500 000 Kč.

Zraněna: 1 osoba. Evakuována: 1 osoba.

10. 11. • Skladová hala náhradních dílů pro osobní automobily,

Český Dub, okr. Liberec.

Příčina: v šetření. Škoda: 12 000 000 Kč.

Zraněn: 1 hasič. Evakuováno: 6 osob.

14. 11. • Sklady a truhlárna v bývalém cukrovaru firmy ITT TRADE, a.s.,

Zákolany, okr. Kladno.

Příčina: úmyslné zapálení.

Škoda: 40 000 000 Kč.

Zraněn: 1 hasič.

26. 11. • Výrobní a skladová hala firmy INTERRA, a.s., Nučice,

okr. Praha-západ.

Příčina: chemické samovznícení v laboratoři.

Škoda: 20 000 000 Kč.

Zraněny: 2 osoby. Zachráněny: 2 osoby. Evakuováno: 16 osob.

7. 12. • Skladová hala dřeva a podlahovin více firem, Luleč, okr. Vyškov.

Příčina: v šetření. Škoda: 19 000 000 Kč.

Zraněna: 1 osoba.

22. 12. • Tkalcovna firmy MILETA, a.s., Hořice, okr. Jičín.

Příčina: technická závada zářivkového svítidla.

Škoda: 250 000 000 Kč.

Zraněn: 1 hasič.

30. 12. • Sklad osiva firmy HORÁKOVA FARMA, a.s., Čejč, okr. Hodonín.

Příčina: úmyslné zapálení.

Škoda: 13 230 000 Kč.

Nejvýznamnějším a nejrozsáhlejším požárem čtvrtého čtvrtletí roku 2012 byl **požár skladu tkalcovny firmy Mileta, a.s., Hořice, okres Jičín**

Každoroční rozsáhlé požáry průmyslových objektů se již v České republice stávají nevídanou tradicí. Charakterizovat je lze zejména nasazením velkého množství sil a prostředků JPO, enormním rozsahem zasažené plochy, významným množstvím ohrožených osob, materiálu nebo technologií vysoké hodnoty, a následně extrémně vysokými škodami způsobenými vlivem požáru, zplodin hoření, zřícených konstrukcí aj. Zásah JPO také často komplikuje složitá orientace v členitém prostředí takového objektu, vnitřní strukturované dispozice jednotlivých budov, přítomnost produktovodů, elektrických vedení a zařízení pod napětím, častá přítomnost většího množství nebezpečných, hořlavých nebo výbušných látek apod.

V sobotu 22. prosince 2012 v 5 hodin 55 minut byl na Krajské operační a informační středisko (KOPIS) HZS Královéhradeckého kraje nahlášen požár v areálu podniku Mileta, a.s. v Hořicích. Podnik se specializuje na textilní výrobu s využitím bavlněné příze. Technologie pro procesy od zpracování základní suroviny po expedici finálních výrobků jsou umístěny v hale o celkovém rozměru 70 x 200 x 11m, dispozičně řešené jako jeden požární úsek o dvou nadzemních podlažích.

K evakuaci osob došlo již před příjezdem jednotky. Průzkumem bylo zjištěno silné zakouření prostoru skladu. Již během nasazení prvních útočných proudů došlo k rychlému šíření požáru, zejména kvůli velkému množství uskladněné příze a textilií. Následně byl vypnut elektrický proud v zasaženém prostoru a postupně také v celém areálu podniku. Vedoucí zásahu vzhledem k předpokládanému velkému rozsahu události zřídil štáb a vyhlásil zvláštní - nejvyšší stupeň poplachu. Na místo byla k hašení povolána také výšková technika. Působením velkého žáru se postupně propadla střecha a byly deformovány boční konstrukce zasažené části haly. Lokalizovat požár se podařilo po necelých osmi hodinách od nahlášení události. Následovalo časově náročné dohašování ohnisek. V průběhu tří dnů bylo nasazeno více než 140 hasičů a 36 kusů požární techniky. Ačkoli byly požárem silně poškozeny nebo zničeny prostory přípravný a expedice výrobků včetně části skladovacích prostor, podařilo se zásahem JPO uchránit prostory a technologie zásadní pro chod podniku. Tím bylo umožněno opětovné započítí výroby v horizontu jednoho týdne od události.



Zdroj: MŮ-GR HZS ČR

Přehled velkých požárů se škodou 10 milionů Kč a vyšší za první čtvrtletí roku 2013

4. 1. – **Slévárna vakuového lití firmy KOVOHUTĚ a.s.**, Rokycany – Nové Město.
Příčina: nepředpokládané změny provozních parametrů.
Škoda: 15 000 000 Kč.
9. 1. – **Sklad elektroniky v budově průmyslového areálu bývalého podniku SVIT**
(poškozeno více firem), Zlín.
Příčina: vznícení hořlavin od zářivkového tělesa.
Škoda: 212 000 000 Kč.
Zraněny: 4 osoby.
17. 2. – **Obytný 3 podlažní panelový dům**, Frenštát p. Radhoštěm, okr. Nový Jičín.
Příčina: úmyslné zapálení.
Škoda: 10 000 000 Kč.
Usmrceno: 6 osob.
Zraněno: 12 osob.
Zachráněno: 12 osob.
Evakuováno: 50 osob.
23. 3. – **Skladovací hala a stolárna firmy MEPROX spol. s.r.o.**, Kostelec, okr. Hodonín.
Příčina: v šetření.
Škoda: 10 000 000 Kč.

Zdroj: MV-GŘ HZS ČR

Přehled připravovaných velkých cvičení pro léta 2013 a 2014

2013

Cvičení RESTART 2013

Společnost ČEPS, a.s., ČEZ Distribuce, a.s, a Ministerstvo průmyslu a obchodu od letošního jara společně připravují cvičení s názvem RESTART 2013, které se bude konat v termínu 2. – 4. září 2013.

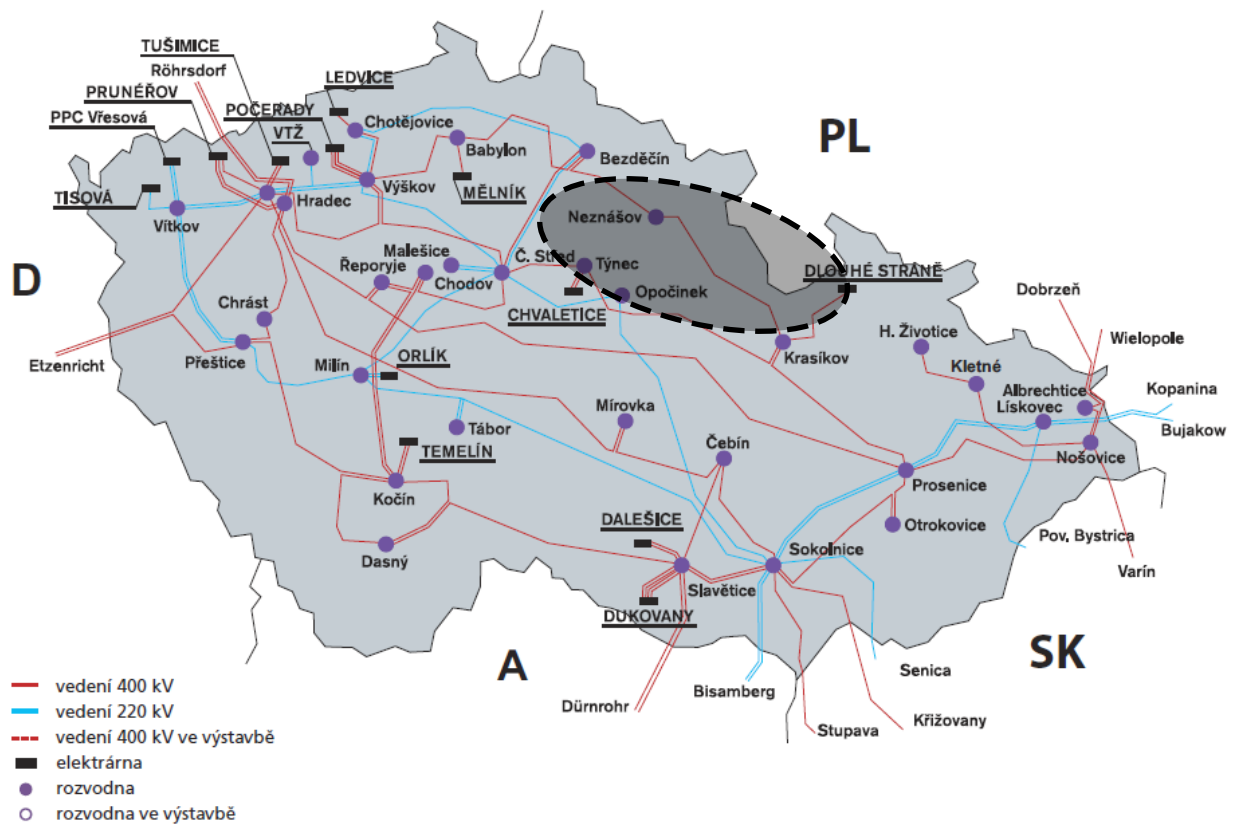
Toto cvičení bude zaměřeno na výpadek elektrického proudu velkého rozsahu (black-out) v oblasti Královehradeckého a Pardubického kraje, který bude způsoben povětrnostními podmínkami (větrná smršť). Dojde k poškození stožáru vysokého napětí a dále vlivem požáru dojde k výpadku vedení na trase Krasíkov – Prosenice. Výpadkem bude postiženo cca 700.000 obyvatel. Dle scénáře cvičení bude zaznamenáno mnoho výpadků na straně výroby v celé Evropě. Evropská síť se rozpadne na několik ostrovů.

Cvičení je koncipováno jako štábní s dynamickým prvkem fyzické výstavby stožárů vysokého napětí pro náhradní trasu vedení. Zúčastní se ho především pracovníci zmíněných společností, složky Integrovaného záchranného systému (IZS), pracovníci dodavatelské firmy, která bude zajišťovat výstavbu náhradní trasy a další subjekty.

Lokální black-out krajů PU a HK

Dynamická část cvičení proběhne z časových důvodů dne 3. září 2013 v katastru obce Železnice (cca 10 km od Jičína). Zde bude fyzicky prováděna stavba stožárů vysokého napětí náhradní trasy. Součástí této části cvičení bude také nehoda pracovníka provádějícího výstavbu (kolaps pracovníka na stožáru). V této části budou aktivně zapojeny především složky IZS.

Dnem „D“ je stanoven termín 4. září 2013, kdy bude probíhat samotné štábní cvičení. Jak již bylo zmíněno, budou cvičit zejména: Operační středisko ČEPS, a.s., ČEZ Distribuce, a.s., složky IZS, Operační středisko GŘ HZS, Operační střediska HZS a P ČR dotčených krajů a další subjekty, hlavně z dopravní sféry. Během cvičení dojde postupně také k výpadku mobilního telefonního spojení (cca po 4 hodinách) a pevného telefonického spojení (cca po 6 hodinách), v důsledku toho bude nezbytné procvičit rovněž komunikace prostřednictvím náhradních zdrojů spojení. Štábní část cvičení bude trvat přes 10 hodin.



Mapa: Zdroj prezentace ČEPS, a.s., ČEZ, a.s.

STEADFAST JAZZ 2013 (SFZJ 2013)

- Mezinárodní cvičení orgánů krizového řízení NATO - cvičení sil rychlé reakce NATO (NRF).
- Tématem je operace NATO vedená podle článku 5 Severoatlantické smlouvy.
- Cílem je procvičit zapojení jednotek vyčleněných do sil NRF a činnosti při plnění úkolu hostitelské podpory (HNS) se zapojením dalších rezortů.
- Cvičení připravuje Ministerstvo obrany, účastní se jej Bezpečnostní rada států, krizové štáby vybraných ÚSÚ, MO a Společné operační centrum NATO.
- Datum cvičení: 27.10. – 7. 11. 2013

BLANÍK 2013

- Cvičení orgánů krizového řízení s tématem ohrožení bezpečnosti civilního letectví.
- Cvičení má za cíl především ověřit metodiku práce OKŘ při řešení mimořádných událostí a získávat poznatky pro zlepšování pracovních postupů a součinnostních vazeb. Dalším z důležitých výstupů cvičení bude zhodnocení reálnosti zpracovaných krizových plánů, typových plánů a jejich příloh, operačních plánů atd.
- Zdůvodnění potřeby tohoto cvičení především vychází z nutnosti i předcházení a řešení protiprávních činů v letectví. To je dáno především tím, že civilní letectví je dlouhodobě terčem útoků teroristů a může být ovlivněno i další trestnou činností (např. pašováním a obchodem s lidmi). Bezpečnostní situace a rizika v oblasti civilního letectví, která by mohla směřovat proti České republice, jsou průběžně sledovány a analyzovány jednotlivými bezpečnostními složkami a pracovními skupinami a tělesy zaměřenými na výměnu informací v této oblasti boje proti terorismu a ochrany civilního letectví před protiprávními činy.

Cvičení připravuje a organizuje Ministerstvo vnitra.

Datum: 25. – 27. 11. 2013

2014

CMX 2014

- Mezinárodní cvičení orgánů krizového řízení NATO.
- Připravuje Ministerstvo obrany, účastní se členské státy a orgány NATO.
- V České republice se cvičení dále účastní: Bezpečnostní rada státu, Ústřední krizový štáb a krizové štáby vybraných ÚSÚ, MO a Společné operační centrum MO.
- Doba provedení: bude upřesněna.



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: listopad 2014.



ROPNÁ NOUZE 2014

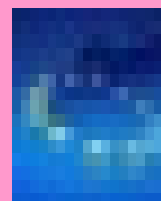
- Společné vnitrostátní cvičení Správy státních hmotných rezerv, vybraných krajů a obcí s rozšířenou působností pro řešení krizové situace Narušení dodávek ropy a ropných produktů do ČR.
- Tématem cvičení je řešení stavu ropné nouze, koordinace činností spojených s problémy se zásobováním pohonnými hmotami, 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 2014.



CME 2014

- Mezinárodní cvičení orgánů krizového řízení EU.
- Tématem cvičení je zvládnání krize civilními a vojenskými prostředky včetně koordinace v rámci EU. Konkrétní námět cvičení se dosud zpracovává.
- Cvičení v ČR organizuje a připravuje Ministerstvo obrany. Účastní se jej: Bezpečnostní rada státu, Ústřední krizový štáb a krizové štáby vybraných ÚSÚ, Společné operační centrum MO.

Doba provedení: bude upřesněna.



Exkurz: Pokračování kauzy metylalkohol v ČR

Kauza otrav metylalkoholem v ČR byla blíže představena v minulém čísle situační zprávy. Nyní se tedy stručně zaměříme na vývoj událostí v první polovině letošního roku.

Tématem metanolu (míněno podezření z trestných činů, jejichž skutková podstata spočívá v tomto konkrétním případě ve výrobě a distribuci potravin/nápojů obsahující zdraví ohrožující, případně nadlimitní obsah látky obecně nazývané metanol) se v rámci Policie ČR zabývá nadále existující tým Metyl, zřízený rozkazem Policejního prezidenta. Trestní řízení (které je ve fázi vyšetřování) je vedeno zejména policejním orgánem Odbor hospodářské kriminality služby kriminální policie a vyšetřování KŘP Zlínského kraje. Dílčí trestní řízení proti některým pachatelům, případně prověřování některých skutků, u kterých nelze dovodit přímou procesní souvislost s osobami „hlavních“ pachatelů, vedou místně a věcně příslušné součásti Policie ČR napříč republikou.

Policie ČR v současné době v metylalkoholové kauze registruje 47 skutků dle § 156 TZ (Ohrožování zdraví závadnými potravinami a jinými předměty), za které stíhá 34 osob. Dále je evidováno 70 skutků dle § 157 TZ (Ohrožování zdraví závadnými potravinami a jinými předměty z nedbalosti), za které je stíháno celkem 31 osob.

Do konce června je evidováno 45 obětí¹³ otravy metanolem a dalších 68 osob bylo hospitalizováno.

V současné době, vzhledem k časovému odstupu a skutečnosti, že je zdroj metanolem kontaminovaných nápojů zjištěn, zadokumentován a nebylo zjištěno nic, co by nasvědčovalo

¹³ 4 osoby z hl.m. Prahy, 1 osoba ze Středočeského kraje, 4 osoby z Jihomoravského kraje, 4 ze Zlínského kraje, 8 osob z Olomouckého kraje, 23 osob z Moravsko-slezského kraje, 1 osoba z Ústeckého kraje. Další oběť přibyla do výčtu dne 16.7.2013 a to ve Středočeském kraji.

tomu, že k výrobě takto kontaminovaných nápojů znovu dochází, probíhá základní preventivní činnost v této oblasti v rámci běžného výkonu služby v gesci jednotlivých Krajských ředitelství policie.

Zdroj: OBP MV, PČR

Exkurz: Povodně 2013

V souvislosti s nepříznivým počasím a extrémními srážkami došlo počátkem června 2013 na území ČR ke vzniku vážné povodňové situace. Situace se vyhroutil nejprve v Jihočeském kraji, poté se začala zhoršovat i ve Středočeském kraji a Praze a následně v kraji Ústeckém. V menší míře byly povodněmi postiženy rovněž Plzeňský, Liberecký a Královéhradecký kraj. Předseda vlády ČR rozhodl 2. června o aktivaci a svolání Ústředního krizového štábu ("ÚKŠ"), jehož předsedou byl jmenován a ústřední koordinací prováděných opatření pověřen ministr vnitra. Od tohoto dne rovněž dle potřeby zasedaly krizové štáby a povodňové komise postižených obcí a krajů. ÚKŠ zasedal během povodní celkem 12x, naposledy 18. června.

V souvislosti s povodněmi byly na území ČR vyhlášeny následující krizové stavy:

- stav nebezpečí (Praha a Jihočeský kraj - od 2. června, 9:45 hod., resp. od 20:00 hod.)
- nouzový stav (Jihočeský, Plzeňský, Středočeský, Liberecký, Královéhradecký, Ústecký a hl. m. Praha - od 2. června, 21:00 hod.)
- *stav nouze v energetice a plynárenství*

Ohrožení v průběhu této mimořádné události bylo dvojího druhu - kromě samotných povodní se vyskytlo velké množství pádů podmáčených stromů, kvůli kterým byla uzavřena řada železničních tratí, a 50 případů sesuvů půdy a skalních masivů (nejznámější byl masivní sesuv půdy na dálnici D8); z tohoto důvodu se zasedání ÚKŠ účastnil i zástupce České geologické služby.

Celkové předběžné náklady na obnovu území krajů (mimo hl. m. Prahu, která má přehled o předběžném odhadu nákladů předložit do 31.7.2013) činí 11 430 799 tis. Kč.¹⁴ Dle odhadů analytiků pojišťoven se výše nahlášených pojistných událostí za letošní povodně bude pohybovat kolem cca 7,5 mld. Kč.

Vláda ČR v červnu rozhodla o uvolnění 300 mil. Kč z kapitoly Veřejná pokladní správa na prvotní platby spojené s řešením povodní pro města a obce (200 mil. Kč z rezerv, 100 mil. Kč z vládní rozpočtové rezervy), na obnovu infrastruktury bylo vyčleněno 3,3 mld. Kč ze Státního fondu dopravní infrastruktury. Na odstranění škod po záplavách v obcích mělo být dle prvotních odhadů zasláno cca 5,3 mld. Kč.

Ministerstvo financí zaslalo v první fázi postiženým krajům 756,8 mil. Kč¹⁵ (Ústecký kraj 323,4 mil. Kč, Jihočeský kraj 70 mil. Kč, Středočeský kraj 220 mil. Kč, Praha 100 mil. Kč, Královéhradecký kraj 30 mil. Kč, Plzeňský kraj 10 mil. Kč, Liberecký kraj 3,4 mil. Kč). Pro fyzické, podnikající fyzické osoby a právnické osoby postižené povodněmi byly schváleny daňové úlevy.

Ministerstvo práce a sociálních věcí vyplatilo 2 740 žadatelům na dávkách okamžité pomoci 23,5 mil. Kč. 600 nezaměstnaných bylo nasazeno na veřejně prospěšné práce související zejména s úklidem po povodních.¹⁶

Správa státních hmotných rezerv ("SSHR") uspokojila během povodní 854 požadavků na věcné prostředky za 187 mil. Kč (např. pohonné hmoty, vysoušeče, vysokotlaké čističe, čerpadla).

¹⁴ Čísla k 17. červenci 2013.

¹⁵ Na financování záchranných prací v době trvání krizového stavu; data jsou k 18. červenci 2013.

¹⁶ Čísla k 18. červnu 2013

Jednotlivým složkám IZS vydala 175 tankovacích karet (HZS 119, PČR 31, AČR 25 karet), na které bylo vydáno 479 tis. litrů benzínu, 494 tis. litrů nafty a 25 tis. litrů leteckého petroleje celkem za 33,1 mil. Kč.

Epidemiologická situace v průběhu povodní zůstala klidná, proti možnému následnému přemnožení komárů byl nakoupen a postiženými kraji aplikován larvicidní přípravek.

Ministerstvo životního prostředí vypracovalo návrh projektu vyhodnocení povodní 2013; vyhodnocení bude zpracováno do poloviny roku 2014 (schválen 3. 7. na schůzi vlády ČR).

Činnost složek resortu MV

Ministerstvo vnitra zpracovalo Krizový manuál pro obce s informacemi pro starosty, kontakty a praktickými radami na řešení různých problémů (*např. postup při vyžadování věcných zdrojů, na který se starostové často dotazovali*), a dne 7. června zajistilo jeho distribuci do postižených obcí.

Dne 2. června v 20:00 hod. spustilo MV psychologickou poradenskou linku "Povodně 2013", kterou zajišťovalo oddělení vedoucího psychologa Policejního prezidia. Tato linka za dobu svého provozu přijala stovky dotazů občanů.

Hasičský záchranný sbor ("HZS ČR") zasahoval během povodní **u 9 600 mimořádných událostí** v 971 poškozených obcích - prováděl evakuaci osob z ohroženého území (**celkem HZS ČR evakuoval 26 438 osob, s pomocí lodí a vrtulníků zachránil 618 osob**), čerpání vody ze zaplavených míst, lagun a později i ze zatopených objektů, vyklízení a demolice havarijně poškozených budov, které ohrožují např. komunikace, dekontaminaci a další odstraňování následků povodní. HZS ČR rovněž na postižených místech poskytoval psychosociální pomoc a jeho příslušníci byli zapojeni do povodňové hlídkové služby.

Celkem bylo nasazeno 28 000 hasičů (profesionálních i dobrovolných), **z toho 3 800 příslušníků HZS ČR. Vynaložené náklady HZS ČR činily** vč. mzdových vícenákladů **70,6 mil. Kč, náklady dobrovolných hasičů** vč. náhrady za ušlý příjem člena jednotky **činily 37,5 mil. Kč.**¹⁷ Na území ČR byla nasazena i pomoc ze zahraničí - dva velkokapacitní čerpací odřady z Polska a Slovenska.

Z centrálních zásob HZS ČR byl ve dnech 2. - 26. června vydán spotřební materiál za 4,6 mil. Kč., zapůjčené prostředky za 52 mil. Kč (např. 115 642 protipovodňových pytlů, 71ks plničků, 3 574 vysoušečů, 9 898 litrů desinfekčních prostředků).

Policie České republiky ("PČR") v průběhu povodní zajišťovala úkoly v oblasti dopravy a bezpečnosti osob, podílela se na evakuaci a řízení dopravy (dopravní opatření na uzavřených komunikacích), hlídala evakuované oblasti, aby v nich zabránila rabování, monitorovala případné sesuvy půdy a další úkoly. Letecká služba PČR průběžně monitorovala situaci, vypomáhala při evakuaci osob z již zaplaveného území a prováděla také kontrolní prohlídky již evakuovaných oblastí s pomocí termovize.

Celkem bylo k řešení povodňové situace nasazeno 694 policistů navíc (ostatní policisté potřebné činnosti zajišťovali v rámci běžného výkonu služby).

PČR spolupracovala s **Armádou ČR ("AČR")**, která **vyčlenila 300 vojáků** k plnění úkolů PČR (celkem se na odstraňování škod po povodních, výstavbě protipovodňových opatření a stavbě náhradních přemostění vystřídalo cca 10 000 vojáků). Na přání prezidenta republiky ČR bylo rovněž **nasazeno 60 příslušníků Hradní stráže ČR**, jež byli využiti především ke střežení majetku a provádění úklidových prací.

PČR v souvislosti s povodněmi evidovala k 18.6.2013 celkem **13 zemřelých osob** (5x vodáci sjíždějící rozvodněné toky, 1x pád do odtokové roury kanálu a následné úmrtí, 3x jiné utonutí ve vodním toku, 2x úmrtí následkem zřícení podmáčené chaty, 1x úmrtí po pádu podmáčeného stromu v parku - *do parku byl zakázán vstup*, 1x úmrtí zasažením elektrickým proudem při výměně pojistek transformátoru v zatopené oblasti - *nedodržení pracovního postupu*), 2

¹⁷ Čísla k 26. červnu 2013

pohřešované osoby (vodáci) a **29 trestných činů** (23x rabování, 1x fyzické napadení, 1x porušení povinnosti při hrozivé tísni, 4x krádež).

Tabulka počtu úmrtí osob v souvislosti s povodní (po jednotlivých dnech)

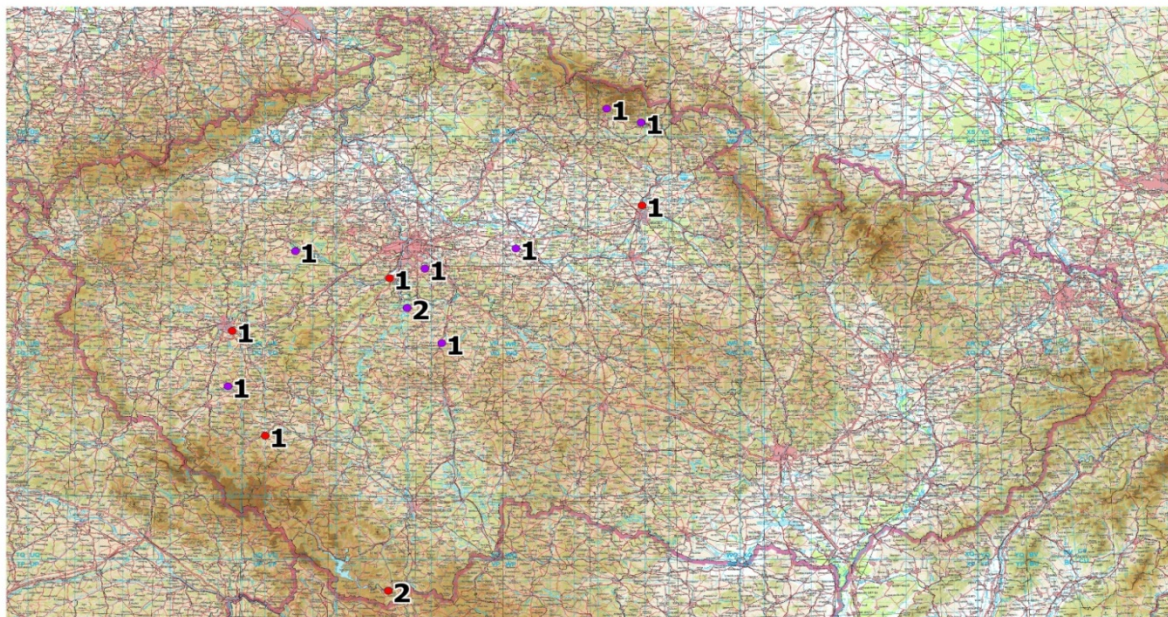
Datum	31. května	2. června	3. června	4. června	7. června	10. června	14. června	16. června	21. června
Počet úmrtí	1	4	2	1	2	1	1	1	2

Tabulka počtu úmrtí osob v souvislosti s povodní (po jednotlivých krajích)

KŘP	Počet	Nález
Středočeský kraj	2	Třeбенice, ÚO Praha - venkov -jih: podmáčená chata.
	1	Průhonice, ÚO Praha- venkov – jih: pád podmáčeného stromu.
	1	Černošice, ÚO Praha - venkov - západ: vodák utonulý v řece Berounce.
	1	Lašovice, ÚO Rakovník: utonulý v Lašovickém potoce.
	1	Olbramovice, ÚO Benešov: utonulý v potoce Cerhenice,
	1	ÚO Kolín: pracovník ČEZ, zásah proudem.
Celkem	7 osob	
Královéhradecký kraj	1	ÚO Trutnov: utonulý v řece Úpě.
	1	ÚO Trutnov: utonulý v řece Malé Labe.
	1	ÚO Hradec Králové: vodák na řece Metuji.
Celkem	3 osoby	
Celkem	3 osoby	
Jihočeského kraje	2	Hebertov, ÚO Český Krumlov: převržený raft na řece Vltavě.
Celkem	2 osoby	
CELKEM KRAJE	15 osob	

Vizualizace obětí povodní na mapě ČR

OBĚTI POVODNÍ V ROCE 2013



● hazard při sportu
● oběť záplav

Přehled nákladů na obnovu majetku v členění podle vlastníků a krajů ke dni 17. 7. 2013

Kraj/Vlastník	Náklady v tis. Kč						CELKEM
	stát	kraj	obce	podnikatelské subjekty	fyzické osoby nepodnikající	právníkové osoby nepodnikající	
Liberecký kraj	174 925	244 430	145 417	1 460	1 845	332	568 409
Jihočeský kraj	165 251	142 628	1 088 704	531 579	76 727	7 758	2 012 647
Plzeňský kraj	23 018	91 708	124 496	25 462	9 355	5 331	279 370
Ústecký kraj	1 027 314	111 267	1 155 786	512 781	707 490	8 470	3 523 108
Středočeský kraj	355 429	1 226 528	1 415 814	389 157	731 467	57 125	4 175 520
Královéhradecký kraj	381 194	106 717	248 295	22 339	112 270	930	871 745
CELKEM	2 127 131	1 923 278	4 178 512	1 482 778	1 639 154	79 946	11 430 799

Přehled nasazení SaP organizační složky HZS ČR v souvislosti s povodní k 6:00 hod dne 18. června 2013											
Poř.	HZS kraje	Celkový počet událostí (od 1. 6. 2013)	Aktuální počet řešených událostí	Celkový počet nasazených JPO od 1. 6. 2013_z toho		Aktuální počet nasazených JPO_z toho		Celkový počet nasazených hasičů od 1. 6. 2013_z toho		Aktuální počet nasazených hasičů_z toho	
				HZS ČR	JSDH O	H Z S Č R	JSDH O	HZS ČR	JSDH O	HZS ČR	JSDH O
1	HZS Středočeského kraje	3062	19	1585	2620	15	20	6306	13112	68	126
2	HZS hl. m. Prahy	1175	3	597	726	2	0	3132	4082	4	0
3	HZS Jihočeského kraje	1336	0	552	784	0	0	1570	2048	0	0
4	HZS Plzeňského kraje	930	0	363	792	0	0	1452	4752	0	0
5	HZS Ústeckého kraje	2356	34	130	359	10	42	1220	3554	38	205
6	HZS Libereckého kraje	114	0	7	83	0	0	88	505	0	0
7	HZS Královéhradeckého kraje	383	0	69	195	0	0	298	1048	0	0
	Celkem:	9356	56	3303	5559	27	62	14066	29101	110	331

Kraj	Počty evakuovaných osob (celkem od 1.6.):															
	3. 6 k 8,00 hod.	3. 6. k 11,00 hod.	4. 6. k 6,00 hod.	4. 6. k 11,00 hod.	5. 6. k 6,00 hod.	6. 6. k 6,00 hod.	7. 6. k 6,00 hod.	8. 6. k 6,00 hod.	9. 6. k 6,00 hod.	10. 6. k 6,00 hod.	11. 6. k 6,00 hod.	12. 6. k 6,00 hod.	13. 6. k 6,00 hod.	14. 6. k 6,00 hod.	15. 6. k 10,00 hod.	16. 6. k 10,00 hod.
Praha	540	710	710	710	1485	1485	1485	1485	1485	1485	1485	1485	1485	1485	1485	1485
Středo- český	1152	2308	3820	5240	6933	7242	7322	8240	8245	8285	8315	8324	8324	8324	8324	12128
Jihočeský	744	744	760	760	763	763	763	763	763	763	847	847	847	847	847	847
Plzeňský	24	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
Ústecký	235	4473	5329	5329	10637	11766	11823	11823	11823	11997	11997	11997	11997	11997	11997	11997
Králové- hradecký	10	10	17	17	17	17	17	17	17	17	17	17	17	17	17	17
Liberecký	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9
Celkem	2714	8279	10670	12090	19869	21307	21444	22362	22367	22581	22695	22704	22704	22704	22704	26508

Tabulka s přehledem nasazených sil (včetně občanských pracovníků)

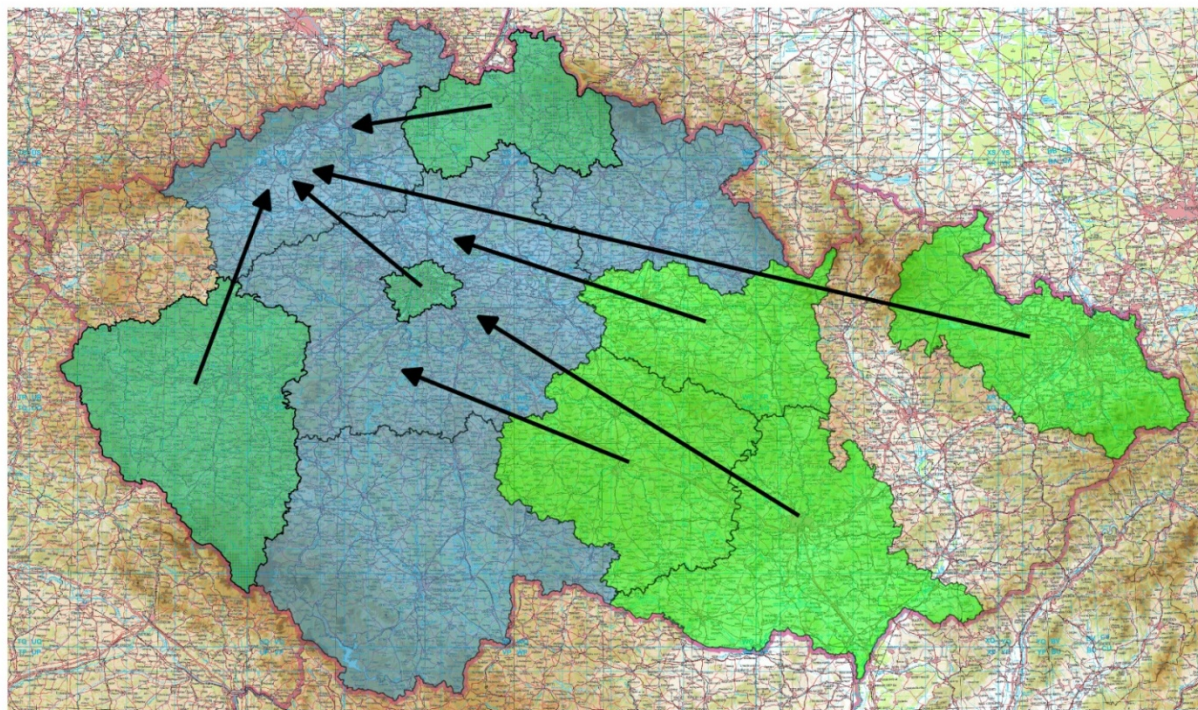
Krajská ředitelství policie	Zkratky	Celkem nasazených policistů do řešení povodňové situace	Celkem nasazených policistů posilujících z jiných KŘP	Celkem Armáda České republiky
Hl. m. Praha	KŘP-A	5534	0	420
Středočeský kraj	KŘP-S	5234	684	650
Jihočeský kraj	KŘP-C	6104	0	0
Plzeňský kraj	KŘP-P	3644	0	0
Ústecký kraj	KŘP-U	4246	373	274
Královéhradecký kraj	KŘP-K	540	0	0
Liberecký kraj	KŘP-L	62	0	0
Celkem		25 364	1 057	1 344

Nasazené síly a prostředky Armády ČR pro posílení Policie ČR



Vizualizace postižených a pomáhajících krajských ředitelství policie v mapě

VÝPOMOC KŘP PŘI POVODNÍCH V ROCE 2013



postižené KŘP
pomáhající KŘP
postižené KŘP poskytující výpomoc

Nasazení vrtulníků Letecké služby Policie ČR

Při povodních byly nasazeny také vrtulníky Letecké služby Policie ČR. Vrtulník letecké služby byl nasazen již 31. května 2013 ve večerních hodinách při pátrání po kajakáři na řece Úslavě, který se převrhl na jezu ve Starém Plzenci, pátrání pokračovalo bezvýsledně i další den v dopoledních hodinách.

Od 2. června 2013 byla na hlavní letecké základně v Praze posílena denní pohotovost o další posádku a vrtulníky. Byla posílena služba leteckých záchranářů HZS. Dále byla na leteckou základnu dislokována speciální jednotka pyrotechniků pro případné nasazení na likvidaci utržených lodí či jiných objektů.

Letecká podpora Policie ČR a HZS byla zaměřena převážně na záchranu a evakuaci osob ze zatopených domů či vodou odříznutých oblastí. **Dne 2. června 2013 bylo evakuováno 10 osob.** Za složitých meteorologických podmínek odstartoval v ranních hodinách vrtulník Bell 412 k evakuaci osob v Krkonoších. V obci Horní Olešnice byla ze zatopeného domu evakuována jedna osoba, další osoby v hotelu v Hostinném evakuaci odmítly. Současně s tím další vrtulník pátral po pohřešovaných osobách podél řeky Berounky od Hlásné Třebáně až po Radotín. V průběhu dne pak vrtulníky Bell 412 evakovaly další osoby ze zaplavených objektů v Miškovcích a Kouřimi, ve večerních hodinách pak proběhla další pátrací akce po pohřešované osobě v řece Metuji v prostou Nového Města nad Metují.

Dne 3. 6. 2013 bylo vrtulníkem Bell 412 evakuováno dalších 6 osob, a to ze zatopené maringotky v Lahovicích, z objektu v Chuchli, chaty v údolí řeky Berounky a budovy v Dolanech. Některé osoby, pro které byl vyslán vrtulník, však evakuaci odmítly. Vrtulník EC-135 prováděl monitorování povodí Vltavy a Labe s pracovníky krizového štábu, pátral po osobě podél řeky Berounky od Černošic až po Radotín.

Od 4. 6. 2013 byla prováděna převážně monitorovací činnost k zjištění aktuálního stavu zaplavených oblastí a průjezdnosti komunikací dle požadavků OO PP ČR nebo požadavků operačních středisek HZS, s pracovníky krizových štábů byla prováděna kontrola protipovodňových opatření a hrází na Vltavě a Labi v okolí Mělníka, ale i stavu říčky Mrliny na Nymbursku. Postupně byl sledován i postup povodňové vlny na Labi od Mělníka přes Roudnici, Litoměřice, Ústí nad Labem, Děčín a Hřensko. V nočních hodinách byly realizovány rekognoskační lety k zabezpečení evakuovaných oblastí proti případnému rabování.

Ke dni 24. 6. 2013 realizovala letecká služba v rámci povodní 50 letových misí **s celkovým náletem 76:20 hodin**, z toho **vrtulníky Bell 412** (OK-BYN, OK-BYR a OK-BYS) **s náletem 25:01 hodin a vrtulníky EC-135** (OK-BYD, OK-BYE a OK-BYF) **s náletem 51:19 hodin**.

Zdroj: OBP MV, MV-GŘ HZS ČR, PČR

Vybrané události ve sledovaném období

Leden

Cvičení MODEX Falck v Dánsku

Ve dnech 25.-28.1.2013 se ve výcvikovém středisku Dánské agentury pro mimořádné události (DEMA) ve městě Tinglev na jihu Dánska uskutečnilo mezinárodní cvičení MODEX Falck. MV-generální ředitelství Hasičského záchranného sboru České republiky na toto cvičení vyslalo Traumateam ČR, který byl v posledních dvou letech vytvářen ve spolupráci Ministerstva zdravotnictví, Fakultní nemocnice Brno, MV-generálního ředitelství HZS ČR a HZS hl. m. Prahy.

Námětem cvičení bylo zemětřesení o síle 8,1 stupně Richterovy škály, které postihlo severozápadní pobřeží země Euland. Následkem zemětřesení vznikla desetimetrová vlna tsunami, která těžce zasáhla pobřežní oblasti Eulandu až 30 km do vnitrozemí. Traumateam ČR byl aktivován poté, co operační a informační středisko MV-GŘ HZS ČR obdrželo fiktivní žádost o pomoc státu Euland prostřednictvím Monitorovacího a informačního centra EU. Po svolání a přípravě ve FN Brno byl team připraven k odjezdu po 7 hodinách od obdržení žádosti. Odjezd teamu z Prahy do Dánska proběhl po 14 hodinách od obdržení žádosti. Na místo přijel také Islandský MUSAR modul (modul pro práci ve zřícených budovách), tým koordinátorů EU a MUSAR modul z Velké Británie. 26. a 27.1.2013 plnil Traumateam ČR úkoly dané scénářem cvičení, které byly organizátory průběžně

přizpůsobovány možnostem teamu tak, aby byly plně využity kapacity teamu.



26.1.2013 došlo dle scénáře k fiktivní autobusové nehodě, následný den došlo ke zřícení budov po aftershocku. Mimo tyto dvě hlavní události řešil Traumatteam ČR také další úkoly různého charakteru – příjem osob podezřelých z nákazy infekční chorobou, ošetření muslimské ženy, kontroly léků ze strany místních celních orgánů, způsob nakládání s mrtvými, ošetření pacientů s nejrůznějšími typy zranění atd. Členové českého teamu pracovali také na sutinách.

Po dobu svého působení ošetřil český team 227 pacientů, z toho 84 vážně raněných a 18 raněných svým zraněním podlehl.

Pro Traumatteam ČR byla účast na cvičení neocenitelnou zkušeností, kdy byly prověřeny všechny složky týmu v ne příliš příznivých mrazivých podmínkách zimního Dánska. Cvičení se zúčastnilo celkem 240 účastníků, včetně 36-členného Traumatteamu ČR.

Únor

Kauza Metyl

Státní zemědělská a potravinářská inspekce našla při kontrole v nelegálním skladu společnosti ALTALIMO, s.r.o. v Karlových Varech 320 litrů lihovin bez potřebných dokladů. Na obalech byly etikety Likérky Drak a Milan Kwaczek. Okamžitě zakázala uvádět alkohol do maloobchodní sítě. Inspekce sklad odhalila při pátrání po původu nelegálního alkoholu v maloobchodní síti. Kontrola se uskutečnila za asistence policistů a celníků.

Inspekce ve skladu našla 254 balení s etiketou Likérky Drak a 385 lahví s etiketou společnosti Milan Kwaczek. Provozovatel skladu neměl povinné nabývací doklady a nebyl schopen původ zboží doložit, část lihovin nebyla ani označena výrobní šarží. Provozovatel skladu porušil také další zákon, protože sklad s potravinami a lihovinami neregistroval. Na místě skladoval i nealkoholické nápoje, víno, pivo, cukr, kávu a cukrářské výrobky. Plocha skladu je zhruba 1000 metrů čtverečních. V době kontroly do skladu vnikla voda, takže prostory nezaručovaly hygienické podmínky pro skladování a uvádění potravin na trh a nebyly řádně zabezpečeny před škůdci. Inspekce proto zakázala místo užívat jako sklad. S provozovatelem bude zahájeno správní řízení pro uvedené porušení potravinářského práva.

Etikety Likérky Drak se objevovaly v souvislosti s metylalkoholovou kauzou, při níž od loňského podzimu zemřely už čtyři desítky lidí. Jednatele likérky Pavla Čanigu loni na podzim vyšetřovali policisté, v listopadu však státní zástupce jeho stíhání zastavil, protože podezření vůči němu byla slabá. V lihovinách z jeho výroby se našel smrtící metanol. Problémy měly už i výrobky s etiketou společnosti Milan Kwaczek z Dobré na Frýdecko-Místecku. Inspekce v nich našla denaturovaný líh, který lze objevit jedině v nelegálním alkoholu.

Výbuch plynu a požár v bytovém domě ve Frenštátě pod Radhoštěm

V neděli 17. 2 2013 došlo v časných ranních hodinách k výbuchu plynu a následnému požáru v bytovém domě v ulici 6. Května ve Frenštátě pod Radhoštěm. V té době se v domě nacházelo celkem 18 osob, z nichž 6 při této události zemřelo a 11 bylo hospitalizováno se zraněním, 1 osoba se zraněním hospitalizována nebyla. Z okolních domů bylo evakuováno 50 osob.

Podle svědeckých výpovědí předcházel samotnému požáru mohutný výbuch. Plameny byly nejprve zpozorovány v bytě v prvním nadzemním podlaží a současně v suterénu, kde se nacházel hlavní uzávěr plynu, na němž byl demontován kužel ventilu. Jako jediná příčina vzniku požáru bylo stanoveno úmyslné zapálení. Objekt byla výbuchem natolik staticky poškozen, že musela být provedena celková demolice.

Březen

Konference Červený kohout 2013

Ve dnech 19. a 20.3.2013 se v Hluboké nad Vltavou konal 16. ročník konference s mezinárodní účastí „Červený kohout 2013“.

Jedná se o konferenci, jejímž cílem je výměna zkušeností a poznatků z praxe mezi odbornou veřejností v celém jejím spektru činností (např. projektanti, odborně způsobilé osoby, hasiči, zástupci vysokých škol, obcí, apod.). Tato konference se konala v prostorách Parkhotelu pod

záštitou náměstka generálního ředitele HZS ČR pro prevenci a civilní nouzovou připravenost brig. gen. Ing. Miloše Svobody. Pozvání přijali i hosté z Prezídia Hasičského a záchranného zboru Slovenské republiky a partneři HZS Jihočeského kraje z družebního Košického kraje.

Na letošní konferenci byla přednesena řada přednášek. V úvodu plk. Ing. Petr Chytrý vystoupil s tématem „Certifikát autorizovaného inspektora a požární bezpečnost staveb – poznatky z praxe“, na kterou v dopoledním bloku navázala přednáška Ing. Františka Konečného z Vysoké školy technické a ekonomické z Českých Budějovic na téma „Novela stavebního zákona ve vztahu k požární ochraně“. Mezi dalšími zajímavými přednáškami prvního dne bych zmínil např. přednášky Ing. Lubora Tomance na téma „Praktické zkušenosti se zásobováním požární vodou veřejnými vodovodními řadami“, plk. Dr. Ing. Zdeňka Hanušky na téma „Požáry fotovoltaických zařízení a zásahy jednotek požární ochrany“, Pavla Šinka na téma „Schopnost kabelových systémů zajistit trvalou dodávku elektrické energie pro požárně bezpečnostní zařízení z pohledu CENELEC“, Ing. Josefa Fedorčáka na téma „Automatický systém včasného varování při lesních požárech“ a p. Ivany Nohové na téma „Technické požadavky a požární bezpečnost komínů v projektové dokumentaci“.

Druhý den začal zajímavým blokem přednášek, který se týkal likvidace technických havárií a požárů. Druhý den vystoupili např. plk. Ing. Martin Sviták na téma „Únik čpavku z velkoobjemového chladicího zařízení – poznatky z praxe“, npor. Lukáš Kamenský DiS. Vystoupil na téma „Rozbor požáru plnirny tlakových lahví propan-butanu“, Ing. Václav Kratochvíl, Ph. D. na téma „Praktické zkušenosti ze zkoušek výbuchů tlakových lahví s technickými plyny“, plk. Ing. Jiří Pokorný, Ph.D. na téma „Aplikace lokálního požáru při navrhování stavebních konstrukcí“.

Duben

Prověřovací cvičení "Požár v areálu nemocnice" - 24.4.2013

Jednotky HZS Praha byly vyslány k požáru archivu zdravotnické dokumentace v půdních prostorách pavilónu č. 4 Nemocnice Na Bulovce. Z archivu byly pomocí vyváděcí dýchací techniky zachráněny 2 osoby. Ostatní personál opustil zasažené prostory na pokyn požární hlídky před dojezdem jednotek. Požární hlídka rovněž vypnula přívod energií do zasaženého objektu. Jednotky objekt odvětraly pomocí přetlakové ventilace.



Květen

Březina 2013

Ve dnech 2. - 4. 5. 2013 se ve vojenském prostoru Březina uskutečnilo taktické cvičení složek IZS. Při cvičení byl simulován rozsáhlý lesní požár, do jehož likvidace byly nasazeny monitorovací systém a bezpilotní letadla. Jihomoravské hasiče ke cvičení inspirovaly poznatky, které získali při hašení rozsáhlého požáru u Bzence v květnu roku 2012. Zásah v nepřehledném terénu trval týden a jedním z největších problémů byla právě orientace a monitorování pohybu techniky a lidí.

Cvičení se během dvou dnů zúčastnily čtyři stovky hasičů ze 44 jednotek z Jihomoravského a Olomouckého kraje. Jeho výsledky by měly sloužit jako manuál při hašení rozsáhlých lesních požárů po celé republice.

Cvičení složek integrovaného záchranného systému Olomouckého kraje – požár hradu Helfštýn

Desítky hasičů, policistů a dalších se 15. 5. 2013 podílely na společném cvičení složek Integrovaného záchranného systému na Přerovsku. Dle scénáře vypukl na hradě Helfštýn požár a nebezpečné plameny zde uvěznil desítky osob.

Celkově se na likvidaci podílely jednotky a další prostředky profesionálních stanic Lipník nad Bečvou, Přerov a Olomouc. V místě byl zřízen štáb posílený spojovým vozem pro koordinované předávání informací na krajské operační středisko v Olomouci. V součtu profesionálních i dobrovolných jednotek hasičů zde zasahovalo osm jednotek. Z řad dobrovolníků byly k pomoci povolány jednotky Lipník na Bečvou, Lhota, Osek nad Bečvou, Radslavice a Týn nad Bečvou.

Cvičení mělo za účel procvičit velmi rychlou evakuaci více osob do bezpečí. Ve spolupráci s Policií ČR procvičit i vyhledávání pohřešovaných osob při požáru a následný transport zraněných k další pomoci zdravotníků na místě.

Mezinárodní konference „Riziková budoucnost pro Evropu a ČR: Jsme na ni připraveni?“

Konferenci pořádalo dne 20. 5. 2013 Středisko bezpečnostní politiky CESES Fakulty sociálních věd UK ve spolupráci s Institutem ochrany obyvatelstva Lázně Bohdaneč. Místem setkání odborníků se stal diskusní sál Poslanecké sněmovny Parlamentu ČR. První blok přednášek se týkal problematiky Evropy a světa v pohybu, druhý blok připravenosti na změny (životního prostředí, přírodní katastrofy, možnosti adekvátní reakce a přizpůsobení) a třetí blok ochrany kritické infrastruktury (faktory zranitelnosti kritické infrastruktury – ignorance bezpečnosti, centralizace a globalizace, standardizace) a zajištění energetické bezpečnosti (budování vyváženého energetického mixu, diverzifikace prostředí, decentralizace zdrojů, vytváření „ostrovních systémů“ v regionech, aby bylo možné v případě nutnosti zrušit závislost na ostatních částech energetické sítě).

Letošní Pyromeeting byl věnovaný požární ochraně historických památek

Pyromeeting, konference, která již tradičně doprovází brněnský veletrh PYROS/ISSET (22. – 24. 5. 2013) byl letos věnovaný požární ochraně historických památek. Toto téma si organizátoři zvolili záměrně. Podíváme-li se do minulosti, ničivé požáry mají za následek ztrátu mnoha významných historických památek. Ani statistiky požárů památek nejsou příznivé, od roku 1997 došlo na území ČR ke 245 požárům historických památek a škoda u těchto objektů je vždy velmi vysoká.

Konferenci oficiálně zahájil náměstek generálního ředitele HZS ČR pro prevenci a civilní nouzovou připravenost brig. gen. Ing. Miloš Svoboda. Mezi vzácnými hosty byli například generální ředitel HZS ČR plk. Ing. Drahoš Ryba, prezident Hasičského a záchranného sboru SR, plk. JUDr. Alexander Nejedlý, zástupce primátora města Brna JUDr. Rostislav Obrlík nebo náměstek pro památkovou péči generálního ředitelství Národního památkového ústavu, Mgr. Martin Tomášek, PhD.

Na konferenci vystoupili přednášející z řad HZS ČR, odborníci v oblasti požární prevence i vědy a výzkumu spolu s experty z Národního památkového ústavu.

Součinnostní cvičení „VODA 2013“

Ve dnech 28. až 30. května 2013 se uskutečnilo součinnostní cvičení „Voda 2013“ v prostorách ČEZ Energetické služby, Ostrava - Vítkovice. Cvičení proběhlo ve spolupráci Ministerstva zemědělství s Krajským úřadem Moravskoslezského kraje, Správou státních hmotných rezerv, ochraňovatelem pohotovostních zásob společností Severomoravské vodovody a kanalizace Ostrava, a.s., a společností TESLA, akciová společnost.

Cílem součinnostní cvičení „Voda 2013“ bylo prověřit systém nouzového zásobování pitnou vodou.

Zdrojem surové vody byla retenční nádrž, rameno řeky Ostravice, která se nachází v areálu ČEZ Ostrava – Vítkovice. K úpravě surové vody z povrchového zdroje byla použita mobilní úpravná vody VIWA 5 HLS, která je v majetku Správy státních hmotných rezerv ČR a je ochraňovaná a udržovaná společností Severomoravské vodovody a kanalizace Ostrava, a.s.

V rámci cvičení provedli zástupci společnosti TESLA, a.s. proškolení pro odbornou obsluhu mobilní úpravné vody VIWA 5 HLS určených pracovníků z Moravskoslezského kraje.

Dohoda o spolupráci hasičských a policejních expertů

Technický ústav požární ochrany zastoupený ředitelem plk. Ing. Zdeňkem Rážem a Kriminalistický ústav Praha zastoupený ředitelem Ing. Pavlem Kolářem, CSc., podepsali 30. května 2013 Dohodu o spolupráci.



Předmětem dohody je spolupráce při

- a. řešení dílčích úkolů (problémů) v rámci
 1. projektů výzkumu, vývoje a inovací z programu Bezpečnostní výzkum Ministerstva vnitra na základě prováděcího protokolu k této dohodě s konkrétní specifikací spolupráce,
 2. laboratorního zkoumání vzorků z místa požárů pro potřeby vypracování znaleckých posudků nebo odborných vyjádření, a to na základě písemné žádosti ředitele jedné ze stran,
 3. mezilaboratorních porovnávacích zkoušek organizovaných jednou ze stran, pro které má druhá strana odpovídající materiálně – technické a personální vybavení, a to na základě písemné žádosti strany organizující tyto zkoušky,
- b. organizování odborných instrukčně metodických zaměstnání, seminářů, konferencí a stáží v souvislosti s problematikou výzkumu, vývoje a inovací, znaleckou činností nebo zjišťování příčin požárů,
- c. publikování vědecko-technických poznatků získaných při vzájemné spolupráci na základě písemného souhlasu obou stran,
- d. vzájemné výměně aktuálních vědecko-technických poznatků a informací o nových přístrojích využitelných při výkonu znalecké činnosti v oblasti požárů a výbuchů s následkem požáru.

Dohoda byla uzavřena na dobu neurčitou a vzájemná spolupráce bude každoročně vždy k 31. prosinci vyhodnocena a do 31. ledna následujícího roku konkretizovány úkoly s termíny plnění pro nový kalendářní rok.

Červen

Součinnostní cvičení „NÁKAZA 2013“

Součinnostní cvičení „Nákaza 2013“ se uskutečnilo ve dnech 11. až 13. 6. 2013 ve vojenském újezdu Libavá (Zemědělská správa VLS Heroltovice – Olomoucký kraj). Cvičení bylo organizováno Státní veterinární správou ČR (SVS) a Vojenskou veterinární službou (VVS) AČR - ÚVVetÚ Hlučín ve spolupráci s Ministerstvem zemědělství a Státní veterinární a potravinovou správou SR (ŠVPS SR).

Cílem cvičení byla praktická činnost Státní veterinární správy ČR ve spolupráci s Vojenskou veterinární službou AČR v místě podezření z nebezpečné nákazy a v primárním ohnisku nebezpečné nákazy s prověřením reálnosti zpracovaného pohotovostního plánu.

Na cvičení proběhly následující činnosti: součinnost orgánů veterinární správy a veterinární služby AČR v případě podezření a potvrzení nákazy SLAK (slintavka a kulhavka) v hospodářství, praktická ukázka činnosti epizootologické skupiny v hospodářství s podezřením na SLAK, praktická ukázka vybavení a činností Ústavů veterinárního lékařství (ÚVL) při podezření na antrax, praktická ukázka vybavení a činností ÚVL při podezření na nebezpečnou nákazu drůbeže, problematika nálezů koní, ukázky vybavení a praktických činností zásahových skupin veterinární služby AČR v místě podezření na nebezpečnou nákazu, vybavení pro imobilizaci zvířat, ukázky vybavení polních laboratoří AČR, ukázky činnosti PSMS (Pohotovostní středisko pro mimořádné situace) v ohnisku nebezpečné nákazy a statická ukázka vybavení ŠVPS SR pro eradikaci ohnisek nebezpečných nákaz.

Cvičení VLAK 2013

19. června proběhla v depu kolejových vozidel Česká Třebová-Rybník, závěrečná část součinnostního cvičení složek Policie České republiky a Integrovaného záchranného systému Pardubického kraje pod názvem „VLAK 2013“, které nařídil hejtmán Pardubického kraje a předseda Bezpečnostní rady Pardubického kraje JUDr. Martin Netolický, Ph. D. v souladu s usnesením bezpečnostní rady Pardubického kraje ze dne 30. ledna 2013. Námětem dvoudenního cvičení byla hrozba likvidace členů společenství „Apokalypsa 2012“ ze strany vedení této skupiny, jejímž motivem bylo udržení majetku převedeného od členů před předpokládaným koncem světa 21. prosince 2012. Tyto členy společně s dalšími rukojmími zadržovali vedoucí představitelé společenství v železničním vagónu. Celé cvičení provázelo krizové vyjednávání vyškolenými odborníky z řad policie, které předcházelo zákroku v místě události.

Do cvičení se zapojilo více než 260 osob.

Byli to policisté Krajského ředitelství policie Pardubického kraje, jeho pořádkové jednotky, příslušníci Útvaru rychlého nasazení - policejní jednotky s celorepublikovou působností, zdravotníci, hasiči, ale i mnoho dalších pomocníků, zajišťujících samotnou organizaci cvičení.



Čeští hasiči jsou již po šesté mistry Evropy v TFA (Toughest Firefighter Alive)

Ve dnech 7. – 8. června 2013 se v německém Mönchengladbachu uskutečnilo dvoudenní mistrovství TFA Germany / Europe, na které vyrazila i česká reprezentace v TFA.

Kromě toho, že jsme se stali mistry Evropy v kategorii do 40 let a v kategorii nad 40 let, jsou čeští borci také absolutními mistry letošního klání.

Disciplíny byly standardní, na prvním stanovišti se roztahovaly a motaly hadice; v dalším desetiminutovém intervalu závodník nastoupil ke kladivu, tunelu s barelem, tahání figuríny a přeskočení bariéry. Jako třetí stanoviště byly připraveny dva žebříky, výstup na schody s barely, vytahování hadic na laně a šroubování konce proudnice. Závěrem čekal na soutěžícího výstup do 14. patra místní nemocnice a zasloužený výhled na město.

TFA TORUŇ (Firefighter's Combat Challenge) - Česká reprezentace přivezla zlatou medaili

Mezinárodního mistrovství Polska v TFA a Combat Challenge s účastí zahraničních družstev USA, Kanady, Francie, Německa, Rakouska, Slovinska, Slovenska, Maďarska a Litvy, které se konalo 27. až 29. června 2013 v Toruni v Polsku, se zúčastnili i dvě desítky závodníků z české TFA reprezentace.

O co se v praxi jedná – v první disciplíně závodník vybíhá s hadicí do věže z lešení, kam po doběhnutí vytahuje závaží. Následně seběhne dolů, kde se ujímá kladiva u „keiser boxu“, aby následně (stále běží v kuse) vyběhl na překážkovou trať, oběhl několik kusů hasičích přístrojů a začal roztahovat zavodněnou hadici. Když s ní následně proběhne dveřmi jako do westernového baru, jeho úkolem je trefit správně mířeným proudem terč a poté ho už čeká jen figurína, kterou táhne několik desítek metrů do cíle.

V další disciplíně musí v historickém centru města roztáhnout a smotat hadice a následně přejít ke druhému úkolu – figuríně. Závodníci se museli přes figurínu převalit a mezitím ji správně uchopit. Proběhnutí s barely tunelem a přezení bariéry bylo již jen standardem. Postavit žebříky, vynést barely do věže, vytáhnout závaží, snést barely opět dolů a našroubovat část proudnice. Na závěr už „jen“ 400 metrový běh k věži a výběh až na její vrchol.



NOVINKY V LEGISLATIVĚ ZA SLEDOVANÉ OBDOBÍ



Energetika a energetická bezpečnost

168/2013

Zákon, kterým se mění zákon č. 157/2009 Sb., o nakládání s těžebním odpadem a o změně některých zákonů

165/2013

Vyhláška o druzích ropy a skladbě ropných produktů pro skladování v nouzových zásobách ropy, o výpočtu úrovně nouzových zásob ropy, o skladovacích zařízeních a o vykazování nouzových zásob ropy

161/2013

Zákon, kterým se mění zákon č. 189/1999 Sb., o nouzových zásobách ropy, o řešení stavů ropné nouze a o změně některých souvisejících zákonů (zákon o nouzových zásobách ropy), ve znění pozdějších předpisů

118/2013

Vyhláška o energetických specialistech

Informační technologie a kyberbezpečnost

73/2013

Vyhláška, kterou se mění vyhláška č. 486/2005 Sb., kterou se stanoví výše a způsob úhrady efektivně vynaložených nákladů na zřízení a zabezpečení rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv, na uchovávání a poskytování provozních a lokalizačních údajů a na poskytování informací z databáze účastníků veřejně dostupné telefonní služby

Krizové řízení

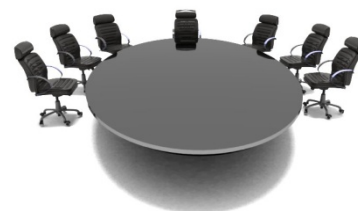
83/2013

Zákon o označování a sledovatelnosti výbušnin pro civilní použití

74/2013

Vyhláška, kterou se mění vyhláška č. 474/2002 Sb., kterou se provádí zákon č. 281/2002 Sb., o některých opatřeních souvisejících se zákazem bakteriologických (biologických) a toxinových zbraní a o změně živnostenského zákona

KONFERENCE A SETKÁNÍ



Energetika a energetická bezpečnost

19. – 21. 11. 2013 For Electron 2013 - Mezinárodní veletrh elektrotechniky, elektroniky a energetiky
PVA Expo Praha Letňany
<http://www.electroncz.cz/2013/cz/intercept.asp>

Bezpečnost finančních institucí

13. – 14. 7. 2013 AML Anti-Money Laundering
Prevence, detekce a vyšetřování praní špinavých peněz
<http://www.business-continuity.cz/aa-27-aml-anti-money-laundering---prevence-detekce-a-ucinne-ws-etrovani-prani-spinavych-penez.php>
8. 10. 2013 Svět informatiky ve finančnictví
Odborná konference je určena pro IT pracovníky a zástupce managementu ve finančním sektoru. Přináší přehled řešení, která umožňují společnostem v této oblasti zefektivnit množství interních procesů, zavádět inovativní obchodní modely a uchovat bezpečnost citlivých dat a informací.
Kongresové centrum U Hájků, Praha
<http://financnictvi.expo-net.cz/>
1. – 3. 11. 2013 Finance pro každého
Veletrh informací z finančního trhu
Olomouc, výstaviště Flora
<http://www.flora-ol.cz/view.php?cisloclanku=2012090001>

Informační technologie a kyberbezpečnost

5. 11. 2013 Cloud Computing Conference
Model Cloud computingu změnil ve světě informačních technologií zažité postupy a obchodní modely. Konference se věnuje jeho možnostem, novinkám a souvisejícím tématům: software jako služba, platforma jako služba, infrastruktura jako služba, virtualizace, datová centra.
Kongresové centrum U Hájků, Praha (2. termín)
<http://ccc.exponet.sk/>
<http://www.cloudconference.cz/>

11. 7. 2013 **Svět informatiky ve zdravotnictví**
Odborná konference je určena pro pracovníky zodpovědné za řízení IT infrastruktury v zdravotnických zařízeních a souvisejících odvětvích. Zabývá se problematikou IT bezpečnosti, využití moderních nástrojů pro automatizaci, komunikaci a zvyšování efektivity procesů v tomto sektoru.
Kongresové centrum U Hájků, Praha
<http://zdravotnictvi.expo-net.cz/>
17. – 21. 9. 2013 **FS Days – Prague Fire & Security Days 2013**
5.ročník mezinárodního veletrhu nejnovějších trendů protipožární a zabezpečovací techniky, systémů a služeb
Téma: „Digitální bezpečnost“
PVA Expo Praha
www.fsdays.cz
19. 9. 2013 **Data Storage Workshop**
Data Storage Workshop nabízí možnost představit IT managerům a IT profesionálům produkty, služby a řešení v oblasti zálohování, ukládání, archivace, bezpečnosti a správy dat, networkingu.
Kongresové centrum U Hájků, Praha
<http://www.dsw.cz/>
22. 10. 2013 **Bezpečnost a dostupnost dat**
Čtvrtý ročník konference nabídne přehledku bezpečnostních produktů, díky kterým zůstane důvěryhodnost, dostupnost a integrace informací zpracovávaných a uchovávaných ve Vašich informačních systémech zachována.
Hotel Crown Plaza, Bratislava
<http://bdd.exponet.sk/>
- podzim 2013 **Security Upgrade 2013**
Bezpečnost informačních technologií, nové trendy
Hotel Diplomat, Praha
<http://www.konferenceit.cz/html/security-upgrade-2013.html>

Krizové řízení

4. – 5. 9. 2013 Sdružení požárního a bezpečnostního inženýrství
XXII. ročník mezinárodní konference Požární ochrana 2013
Clarion Congress Hotel Ostrava
<http://www.vsb.cz/info/?&lang=cs&block=simple&reportId=15948&showExpired=true&showExpired=true>
6. – 8. 9. 2013 **Tři dny se záchranářů**
12. ročník akce představující Integrovaný záchranný systém. Výstava moderní policejní a požární techniky.
Lysá nad Labem, areál výstaviště
<http://www.vll.cz/veletrh-146>
25. – 27. 9 2013 **Medicína katastrof**
16.ročník mezinárodní konference
Téma konference: Reakce státní správy a samosprávy na mimořádné události
Uherské Hradiště, prostory Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně
www.medicinakatastrof.cz

11. – 12. 11. 2013 CityPlan, pod záštitou ministra dopravy a ředitele služby dopravní policie
8. ročník mezinárodní konference Bezpečná dopravní infrastruktura 2013
<http://konference.cityplan.cz/>

Připravované akce v zahraničí

Energetika a energetická bezpečnost

29. – 31. 10. 2013 **Power Kazachstan 2013**
Mezinárodní energetický veletrh s oficiální účastí ČR
Almaty, Kazachstán
<http://www.exponet.ru/exhibitions/by-id/powerkazal/powerkazal2013/index.en.html>

Informační technologie a kyberbezpečnost

27. 7. – 1. 8. 2013 **Black Hat USA 2013**
Konference o kybernetické bezpečnosti a fenoménu hackingu
Caesars Palace, Las Vegas, USA
<http://www.blackhat.com/us-13/>

Krizové řízení

17. – 19. 9. 2013 **SAFE**
Konference pokrývá oblasti, jako je krizové řízení, bezpečnostní inženýrství, přírodních katastrof a mimořádných událostí, terorismus, bezpečnosti IT, člověkem způsobených katastrof, řízení rizik, řízení, ochrany a zmírňování problémů, a mnoho dalších.
Řím, Itálie
http://expopromoter.com/cs/events/138645/safe_2013/
30. – 31. 7. 2013 **ICCTHS 2013 : International Conference on Counter Terrorism and Human Security**
Vědecká konference týkající se výměny zkušeností a vědeckých výzkumů ohledně témat Counter Terrorism and Human Security.
<https://www.waset.org/conferences/2013/switzerland/iccths/index.php>
25. – 30. 10. 2013 **IAEM 61st annual conference and EMEX**
Konference se bude týkat témat vnitřní bezpečnosti a pohotovostního managementu. Určena je pro všechny vládní úrovně, soukromý sektor a sektor veřejného zdraví za účelem spolupráce při ochraně života a majetku.
Silver Legacy Hotel and Reno Events Center, Reno, Nevada, USA
Informace o možnostech účasti a vízech:
<http://www.iaem.com/events/annual/intro.htm>

Zdroje použité pro monitoring

MV, PČR, MV-GŘ HZS ČR, MPO, MO, MZV, ČTK, vlada.cz, ceps.cz, cez.cz, energetickakoncepce.cz, prumysl.cz, ČT 24, ČRo, net4gas.cz, ceprs.com, banktech.com, lidovky.cz, euraktiv.cz, europa.eu, ihned.cz, idnes.cz, eset.cz, computerworld.cz, mcafee.com, isis-europe.eu, konference.org, novinky.cz, tyden.cz, policista.cz, mesec.cz, forum2000.cz, bvv.cz, counterterrorexpoc.com, eur-lex.europa.eu, denik.cz, csob.cz, root.cz, labs.nic.cz, govcert.cz, cesnet.cz, saferinternet.cz, bezpecnyinternet.cz, ceskenoviny.cz, zpravy.tiscali.cz, radyvnouzi.cz, portal.gov.cz, konferenceit.cz, security-portal.cz, cbss.cz, iir.cz, sbp.fsv.cuni.cz, vojenskaskola.cz, mup.cz, veletrhyavystavy.cz, blackhat.com, banksecurityportal.com, business-continuity.com, pro-energy.cz, energetika.cz, euroexpo.cz, europeum.org, cybersecurity.cz

Zdroje obrázků

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.