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. září do 31. prosince 2012

Odbor bezpečnostní politiky Ministerstva vnitra

leden 2013

OBSAH

ÚVODEM

Vážení čtenáři,

dostává se Vám do rukou periodická situační zpráva, která mapuje vybrané oblasti bezpečnosti v závěrečné části roku 2012. Těmito vybranými oblastmi jsou: energetická bezpečnost, bezpečnost finančních institucí, kybernetická bezpečnost a informační kriminalita a krizové řízení. Tuto zprávu zpracovává odbor bezpečnostní politiky Ministerstva vnitra.

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

Každé výše uvedené oblasti je věnována samostatná kapitola, která vždy obsahuje výběr nejdůležitějších událostí, k nimž ve sledovaném období došlo (se stručným popisem každé z nich) a dále statistická data, týkající se především kriminality a mimořádných událostí v probíraném sektoru. Zdrojem těchto údajů jsou zejména Policie České republiky a Hasičský záchranný sbor. Kromě samotných tabulek a čísel nechybí v této části ani určitá interpretace a analýza hlavních trendů současnosti, včetně výhledů do budoucna. Mimo sledované období jsou často připojena i data za celý rok 2012.

Některé kapitoly jsou rozšířeny o podrobnější analýzu souvisejících fenoménů. V případě energetické bezpečnosti je tak zvláštní oddíl věnován obsahu a kritice připravovaných strategických dokumentů, které by měly určovat podobu tohoto odvětví v budoucích letech (jedná se o Státní energetickou koncepci, Surovinovou politiku ČR a velkou novelu horního zákona). Je zde možné nalézt i odkazy na plné znění těchto materiálů.

V sekci o kybernetické bezpečnosti a informační kriminalitě čtenář nalezne oddíl zvlášť věnovaný očekávaným bezpečnostním hrozbám a trendům pro nadcházející rok 2013. Tento výhled upozorňuje na hlavní rizika, jejichž široký výskyt je možné v blízké budoucnosti očekávat, a na která je nutné se připravit. Kapitola o krizovém řízení je naopak rozšířena o přehled připravovaných velkých cvičení v nadcházejících dvou letech.

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 uplynulém roce 2012. Z policejních statistik se zde dozvídáme, že celkový počet zaznamenaných trestných činů (304 528) meziročně poklesl o 4% a je tak nejnižší od první poloviny 90. let. Zatímco např. násilná či mravnostní kriminalita dále klesala, některé formy zločinu (např. ty prováděné v kyberprostoru) doznaly naopak značného nárůstu. Pokles celkového počtu trestných činů bohužel nebyl doprovázen poklesem výše škod při nich způsobených – ty naopak poměrně značně vzrostly.

Konkrétnější data je možné nalézt v následujících kapitolách věnovaných jednotlivým oblastem bezpečnosti. Z údajů policie věnovaných energetickému sektoru je možné učinit závěr, že v České republice nedochází k téměř žádným cíleným útokům na energetickou infrastrukturu. Největší problémy tak způsobují především různé krádeže (např. vodičů, kabelů, elektroinstalačního materiálu), podvody a samozřejmě nehody a mimořádné události. Do statistik se mimořádně promítla především jedna zásadní událost, a sice požár bývalého objektu odsíření elektrárny Tušimice, kde celková škoda dosáhla výše přes 100 milionů korun.

Součástí této kapitoly je také shrnutí obsahu některých důležitých připravovaných strategických materiálů, především Státní energetické koncepce a Surovinové politiky ČR. Z nich vyplývá především vládní cíl dosáhnout při výrobě elektrické energie 80% soběstačnosti, zdvojnásobit podíl jádra, a naopak radikálně snížit podíl tuhých paliv v energetickém mixu. Surovinová politika ČR zase počítá se ekonomickým využitím dalších strategických surovin, především uranu, zlata, či wolframu.

Kapitola o bezpečnosti finančních institucí zase prezentuje statistiky kriminality cílené na toto odvětví, které trápí především různé formy podvodného jednání. Alarmující je především výše škod (přes tři čtvrtě miliardy korun) v případě úvěrových podvodů během uplynulého roku. Pozitivní zprávou je naopak vysoká objasněnost tohoto typu trestné činnosti, která celkově činí přes 80%. Kapitola je věnována i dalším fenoménům v oblasti bezpečnosti finančních institucí, např. skimmingu či viru Eurograbber.

Další část zprávy se zabývá kybernetickou bezpečností a také samozřejmě kybernetickým zločinem. Ten je jednou z nejrychleji se rozvíjejících forem kriminality – podle policejních statistik zaznamenal počet (nahlášených) trestných činů v této oblasti meziročně více než čtvrtinový nárůst. Lze přitom předpokládat, že se policii daří podchytit jen zlomek celkového objemu nežádoucích aktivit v kyberprostoru, třebaže její možnosti i schopnosti se rok od roku zlepšují. Kapitola se zabývá také činností dalších součástí státní správy při zajišťování kybernetické bezpečnosti, především pak vznikem Národního centra pro kybernetickou bezpečnost a přípravou nového Zákona o kybernetické bezpečnosti. Další část materiálu je věnována očekávaným bezpečnostním hrozbám a trendům pro rok 2013, kde lze předpokládat především další přesun pozornosti zločinců k mobilním technologiím. Text také upozorňuje na rizika skladování dat v cloudu, fenoménu BYOD, či pokročilé formy spear phishingu. Zvláštní oddíl je věnován novému špionážnímu viru, který dostal název Rudý říjen.

Podstatná část kapitoly o krizovému řízení je věnována statistikám Hasičského záchranného sboru a jeho evidenci mimořádných událostí za rok 2012. Zde došlo s počtem 80 894 k mírnému nárůstu oproti roku 2011, ovšem ve srovnání např. s rokem 2007, kdy tento počet překročil 93 000, jde stále o čísla velice příznivá. Kromě výběru připravovaných cvičení se zde nalézá také speciální sekce věnovaná metylalkoholové kauze v České republice, respektive jejímu závěrečnému shrnutí.

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

CELKOVÁ KRIMINALITA V ČR V ROCE 2012

Registrovaná kriminalita v meziročním srovnání

Za období od 1. 1. do 31. 12. 2012 Policie ČR registrovala celkem 304 528 trestných činů (-12 649, -4 %). **To je nejmenší počet od roku 1992**.
Objasněno bylo 120 168 skutků (-2 070, -1,7 %). Počet objasněných trestných činů byl tak druhý nejnižší od roku 1992.

Zjištěná kriminalita meziročně poklesla (-4 %).

Mírně klesl též počet objasněných trestných činů (-1,7 %). Nepodařilo se udržet jeho nastartovaný růst z roku 2011.

Počty zjištěných trestných činů všech hlavních kategorií kriminality poklesly:
- násilná kriminalita (-5,4 %)
- mravnostní kriminalita (-5 %)
- majetková kriminalita (-4,3 %)
- ostatní kriminalita (-2,3 %)
- hospodářská kriminalita (-2,1 %)

Zjištěné škody vzrostly o 42,9 %, zajištěné hodnoty[1] poklesly o 9,5 %.

Celková objasněnost dosáhla 39,5 % a mezi-ročně se zvýšila o 0,9 %.

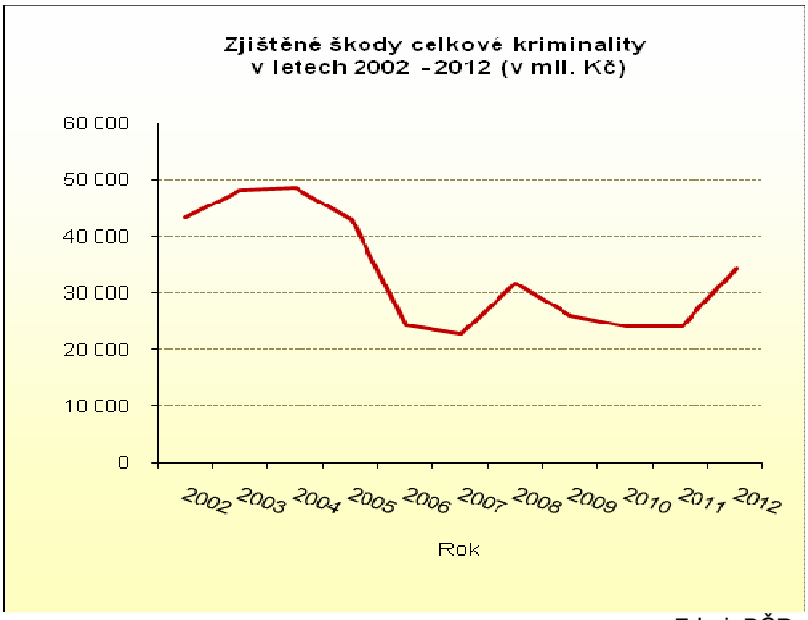
Zjištěné hmotné škody meziročně výrazně vzrostly, a to o téměř 43 % na cca 34,2 mld. Kč (v roce 2011 23,9 mld.) a byly tak nejvyšší od roku 2008. Nárůst zjištěných škod je ovlivněn i zvýšenou aktivitou ÚOKFK PČR, který podal o 92 % podnětů k trestnímu řízení více než v roce 2011.

Na způsobených škodách se v roce 2012 nejvíce podílely trestné činy: krácení daně (916 skutků s 26% podílem na škodách) trestné činy proti předpisům o nekalé soutěži (pouze 38 skutků s 23,3% podílem na škodách) a podvod (4363 skutků s podílem na škodách 20,6 %).

Nicméně ke kulminaci zjištěných škod – od roku skutků s 23,3% podílem na škodách) a podvod (4363 skutků s podílem na škodách 20,6 %).

[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.**

Nicméně ke kulminaci zjištěných škod – od roku 2002[2] – došlo zatím mezi roky 2002 až 2005, jak ukazuje graf 1.



Zdroj: PČR

Vybrané markanty registrované kriminality

Největší meziroční pokles v absolutních počtech byl evidován u krádeží věcí z automobilů (-4 479,-13,5 %). **Krádeže motorových vozidel poklesly o 1244 skutků, tj. (-10,7 %).**

Pokles obou druhů těchto trestných činů je dlouhodobějšího charakteru (krádeže věcí z aut klesají od roku 2009, krádeže motorových vozidel od roku 2004).

Pokračoval pokles krádeží vloupáním do ostatních objektů (-3 800, -10,4 %),[3] jejichž nárůst dominoval v roce 2011. V rámci násilné kriminality nejvíce poklesly loupeže (-478 skutků, tj. -12,7 %).

Pokud se týče hospodářské kriminality, nejvíce poklesl počet trestných činů ochrana měny (-1 173 skutků). **Výrazný více než 20% pokles úvěrových podvodů z roku 2011 nepokračoval, naopak došlo ke změně trendu a jejich nárůstu +6,2 %**.

V absolutních číslech nejvíce vzrostl počet krádeží kapesních (+916, +6,3 %). Druhý nejvyšší nárůst byl zaznamenán u krádeží v jiných objektech (+648, +2,9 %). Do této kategorie jsou zařazovány např. krádeže v prodejních a skladovacích prostorech, výrobních a provozních místech, čekárnách aj. Následují podvody majetkové i hospodářské (+521, +228) a krádeže jízdních kol (+387) a krádeže vloupáním do rodinných domků.

[2] V roce 2002 byla změněna hranice škody nikoliv nepatrné, která při splnění dalších podmínek trestní odpovědnosti určuje, zda se jedná o trestný čin, z 2000,- Kč na 5000, - Kč.

[3] 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.

Stíhané a vyšetřované osoby

Celkem bylo stíháno a vyšetřováno 113 026 osob. Meziročně došlo k poklesu počtu stíhaných a vyšetřovaných osob o cca 1,7 %, což odpovídá poklesu počtu objasněných trestných činů. Celkový meziroční vývoj ukazuje následující tabulka

Počty stíhaných osob v meziročním srovnání

	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	1 568	1,4	1 371	1,2
mladiství 15 až 18 let	4038	3,5	3 486	3,1
ženy	15 260	13,3	15 479	13,7
cizinci	7 473	6,5	7 513	6,6

Zdroj: PČR

Počet recidivistů dále vzrostl na 56 489 (+772, +1,8%) a jejich celkový podíl na stíhaných a vyšetřovaných osobách dosáhl hranice 50 %.

Přetrvává stav, který ukazuje, že současné postupy k nápravě recidivistů nejsou účinné.

Toho důsledkem a příkladem je skutečnost, že v roce 2012 117 recidivistů spáchalo trestný čin vraždy (tj. 57,9 % ze všech osob stíhaných a vyšetřovaných pro vraždy). Recidivisté v roce 2012 spáchali 105 vražd, tj. 55,9 % ze všech zjištěných vražd a 60 % z vražd objasněných.

Další informace a statistiky naleznete ve „**Zprávě o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2012**“, kterou zpracovává rovněž odbor bezpečnostní politiky a naleznete ji na stránkách Ministerstva vnitra www.mvcr.cz.

ENERGETICKÁ BEZPEČNOST

Policejní statistiky a jejich interpretace

Trestné činy za období 1. 1. – 30. 9. 2012 dle „druhu napadených objektů“

druh objektu	zjištěno tr. činů	škody
plynárny	157	9 291 500 Kč
elektrárny	311	51 147 900 Kč
teplárny	79	3 023 700 Kč
energetické závody	541	46 968 900 Kč
tranzitní plynovody	2	64 800 Kč
celkový součet	**1090**	**110 496 800 Kč**

Zdroj: PČR

Z uvedených statistik trestné činnosti za rok 2012 vyplývá, že ve výše zmíněných objektech energetické infrastruktury došlo celkem k více než tisícovce trestných činů, přičemž škody z nich přesáhly částku sta milionů korun.

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 „klasický“ teroristický útok, který by měl za cíl narušit energetickou infrastrukturu v ČR, se ve sledovaném období nestal.

V této souvislosti lze připomenout např. červnový případ výpadku proudu na Novojičínsku. Zloději kovů zde odcizili železné vzpěry stožárů vysokého napětí, které se později pod náporem větru zřítily. Celková škoda přesáhla 12 milionů korun, tisíce lidí se nakrátko ocitly bez elektrické energie. V tomto případě se sice jednalo o narušení dodávek většího rozsahu, to ovšem nebylo pravým cílem pachatelů, kteří byli motivováni čistě zištnými důvody. Policii se nakonec podařilo v říjnu viníky zadržet a byli obviněni z krádeže a z poškození a ohrožení provozu obecně prospěšného zařízení.

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**. Tyto vyjmenované činnosti (krádeže, podvody) **tvoří více než 80% z počtu trestných činů**. Zcela drtivou část celkové kriminality zaujímají také z hlediska výše škod. Zde hrají svou roli také nehody, havárie a incidenty způsobené např. špatným počasím, které se ovšem do policejních statistik nedostávají. Pouze některé z nich policie vyšetřuje pro podezření z nedbalostního trestného činu (to je např. případ výbuchu v koksovně ArcelorMittal).

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. Stejně jako v případě policie máme i od HZS k dispozici souhrn od ledna do září roku 2012 (statistiky za celý rok 2012 se teprve zpracovávají a budou k dispozici v příští situační zprávě a rovněž na stránkách HZS). 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 tu část údajů, která má vazbu k energetické infrastruktuře. Hlavní informace shrnuje následující tabulka:

Požáry v energetických odvětvích hospodářství v ČR od 1. ledna do 30. září 2012

Odvětví	Počet požárů	Podíl v %	Škody v Kč	Usmrcených	Zraněných
Výroba, rozvod el. a plynu	135	0,8	146 795 000	0	6
Těžba nerostných surovin	13	0,08	15 776 000	0	0

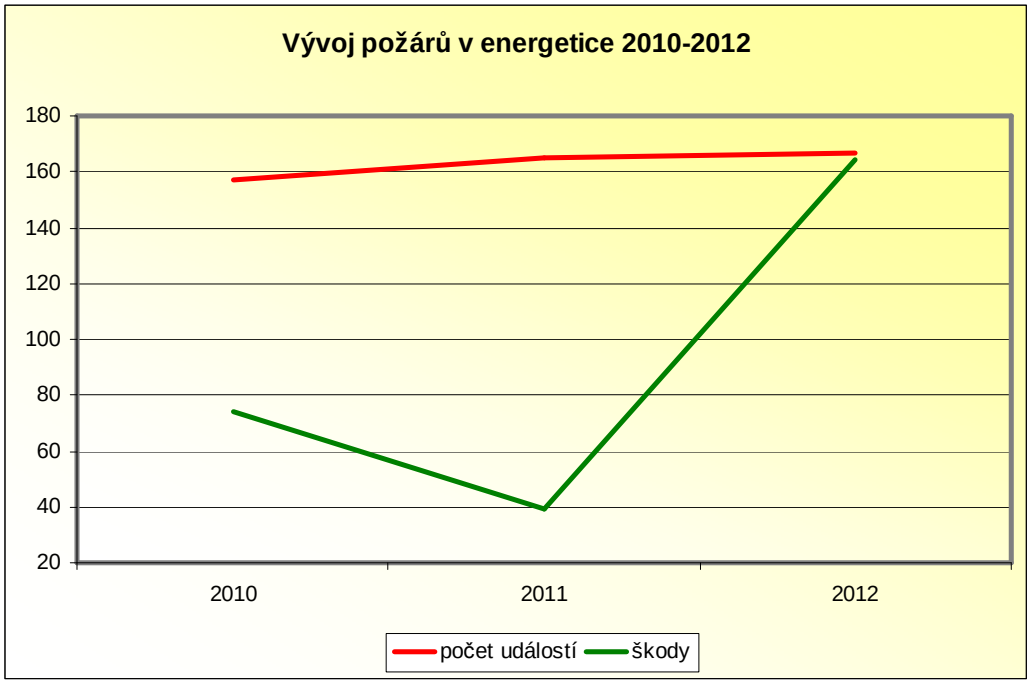
Zdroj: MV-GŘ HZS ČR

V prvních třech čtvrtinách roku vzniklo v České republice celkem 16 793 požárů. Pouhých 0,88% se týkalo výroby a rozvodu elektřiny a plynu, případně těžby nerostných surovin. Škody v těchto dvou odvětvích přesáhly 150 milionů korun, zraněno bylo celkem 6 osob.

Následující tabulka shrnuje požáry (včetně výbuchů na bázi hoření) v odvětví výroby a rozvodu elektřiny, plynu a vody za poslední tři roky (v tomto případě jsou k dispozici data za celý rok 2012). Změny v jednotlivých letech jsou zaznamenány v grafu na následující straně.

rok	2010		2011		2012	
období	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	18,0
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	39,0	167	164,5

Zdroj: MV-GŘ HZS ČR



Z grafu je patrný poměrně stabilní nárůst incidence mimořádných událostí v energetickém sektoru, který lze vysvětlit především nárůstem počtu zdrojů energií (přibývá např. fotovoltaických elektráren). Naopak velká fluktuace škod je ovlivněna zejména velkými požáry se značnou škodou.

V roce 2012 statistiku mimořádně ovlivnila jediná událost, kterou byl **požár haly odvodnění energosádrovce bývalého objektu odsíření elektrárny Tušimice** (poblíž Chomutova), který vznikl 20. července následkem nedbalosti při svařování. **Celková škoda se vyšplhala na 100 milionů Kč**, což z tohoto požáru činí jeden z nejdražších evidovaných incidentů tohoto roku v České republice vůbec, který ve sledovaném období překonává pouze požár hangáru a letadla ATR na Ruzyňském letišti (zde byla škoda půl miliardy Kč). Pro úplnost připojujeme výčet velkých požárů, které v uplynulých třech letech výrazněji zasáhly energetický sektor.

Rok 2010

23. 4. - **Střídač napětí v technologickém kontejneru fotovoltaické elektrárny** firmy EKOSOLAR NICOL, sp
Příčina **:** technická závada – elektrický zkrat.
Škoda : 15 000 000 Kč.

27. 4. – **Dvě trafostanice** firmy ALPIQ GENERATION spol. s.r.o., Kladno.
Příčina : technická závada na olejovém transformátoru VVN.
Škoda : 26 000 000 Kč.
Zraněni : 2 hasiči.

8. 9. **– Turbogenerátor,** SOKOLOVSKÁ UHELNÁ, PRÁVNÍ NÁSTUPCE a.s., Vřesová, okr. Sokolov.
Příčina : výbuch s následným požárem vlivem závady ventilu parovodu.
Škoda : 12 000 000 Kč.
Usmrcena : 1 osoba.
Zraněno : 7 osob.

8. 11. – **Kotelna na LTO** firmy AHV EKOLOGICKÝ SERVIS spol. s.r.o., Stráněice – Svojšovice, okr. Praha východ.
Příčina : technická závada – elektrický přechodový odpor na vzduchovém vypínači.
Škoda : 10 000 000 Kč.

Rok 2011

21. 4. – **Rozvodna fotovoltaické elektrárny**, Vojkovice, okr. Frýdek – Místek. Příčina – technická závada. Škoda – 7 500 000 Kč.

Rok 2012

24. 4. – **Kompenzační transformátor**, Karlovy Vary-Bohatice. Příčina: technická závada. Škoda: 7 000 000 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.

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.

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.

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

Shrnutí obsahu a kritiky připravovaných strategických dokumentů

Budoucí směřování české energetiky je opět o trochu jasnější. Vláda totiž současné době připravuje hned tři zásadní dokumenty, které by měly přinést podstatné změny do energetické politiky ČR. Jedná se o **Státní energetickou koncepci** a **Surovinovou politiku ČR**. Bude proto vhodné se na oba dva tyto strategické materiály podívat podrobněji a ve stručnosti shrnout hlavní změny, které přináší.

Státní energetická koncepce

Velmi významná je především aktualizace Státní energetické koncepce, která se snaží definovat směřování české energetické politiky ve střednědobém a dlouhodobém horizontu. Vláda ji na svém zasedání dne 8. listopadu 2012 vzala na vědomí a v současné době se materiál nachází ve fázi posuzování vlivu na životní prostředí (SEA).

Světová hospodářská krize a vzestup nových mocenských hráčů způsobily, že se strategické suroviny a energetické zdroje stávají v čím dál větší míře předmětem globálního soupeření. Dlouhodobě stabilní dodávky a ceny energií tak lze zajistit pouze prostřednictvím maximální diverzifikace jak z hlediska zdrojů a druhů surovin, tak z hlediska přepravních tras a zdrojových teritorií.

Vzhledem k provázanosti globální ekonomiky je přitom třeba mít na paměti, že některé zahraniční události může Česká republika jen těžko výrazněji ovlivnit, a přitom mohou mít poměrně výrazný dopad na její energetickou bezpečnost (např. rozhodnutí Německa o opuštění jádra, ruská zahraniční politika, bezpečnostní situace ve Střední Asii či v Perském zálivu). Z tohoto důvodu nová strategie opět přistupuje ke zvýšené podpoře domácích zdrojů, jakkoliv ČR i v budoucnu zůstane ekonomikou výrazně závislou na zahraničních dodávkách (zejména ropy a zemního plynu). **Vládním cílem je, aby až 80% elektrické energie pocházelo z domácích zdrojů**.

Zdůrazněno je také aktivní vystupování v EU při formulování celoevropských strategií, při současné snaze zabránit opatřením, která by mohla poškodit konkurenceschopnost českého průmyslu. Koncepce tak kromě důrazu na zvyšování energetické účinnosti a úspory energie zmiňuje i podporu výzkumu a inovací. Celkově materiál počítá s udržením mírně exportního salda v oblasti obchodu s elektřinou a s dalším rozvojem přenosových sítí (včetně tzv. smart grids).

V souladu s výše zmíněnou snahu o maximální možnou energetickou nezávislost klade nová strategie důraz na posílení role jádra při výrobě elektřiny, třebaže některé okolní země nastupují trend právě opačný. Materiál počítá s výstavbou dvou nových bloků v Temelíně a jednoho bloku v Dukovanech, kde má být zároveň prodloužen provoz čtyř stávajících reaktorů. Dokument hovoří i o zahájení příprav na vymezení území pro případnou výstavbu zcela nové jaderné elektrárny – v této souvislosti se hovoří například o Blahutovicích u Jeseníku nad Odrou. **Podíl jádra na energetickém mixu by se tak mohl zdvojnásobit – ze současných 16 procent na 30-35 procent**.

Poměr elektřiny vyrobené z uhlí by se naopak měl postupně snižovat, dosluhující uhelné elektrárny mají být postupně uzavírány, uhlí by se naopak mohlo více využívat v teplárnách, aby byla omezena jejich současná velká závislost na dodávkách plynu. Celkově strategie mluví o maximálním využití odpadního tepla, například také z jaderných provozů. **Podíl tuhých paliv by měl v mixu klesnout ze současných 40% na 12-17%**. K tomu mají přispět i další výměny malých domácích kotlů spalujících uhlí za ty, které využívají elektřinu, plyn či obnovitelné zdroje.

Ačkoliv podíl uhlí v celkovém energetickém mixu má postupně klesat, strategie (a především další dokument – Surovinová politika ČR) nevylučuje, že nakonec dojde k prolomení těžebních limitů a k pokračování těžby. **České zásoby uhlí mají být totiž vyčerpány již kolem roku 2035**.

K prolomení limitů by mohlo dojít jak v případě dolu ČSA, tak u dolu Bílina, přičemž tento krok musí začít být intenzivně připravován nejpozději do roku 2016. Za strategické označuje Ministerstvo průmyslu a obchodu, v jehož gesci nový materiál vznikal, také zásoby v beskydském dole Frenštát, ve kterém by se mohlo nacházet až 1,6 miliardy tun černého uhlí, což jej zřejmě řadí mezi největší dosud nevyužitá ložiska v celé Evropě (srovnatelná či větší se údajně nacházejí zřejmě již jen v ukrajinském Dombasu a v Lublinské pánvi na pomezí Polska, Ukrajiny a Běloruska). Dalších zhruba 1,5 miliardy tun uhlí hnědého se může ještě nacházet na Kladensku a Mělnicku.

V souvislosti se zajištěním maximální surovinové nezávislosti i s plány na ekonomický rozvoj některých regionů uvažují tyto strategické dokumenty i o využití dalších domácích surovin. **Jako velmi perspektivní je zmiňován hlavně uran**, jehož má ČR stále poměrně slušné nevyužité zásoby. Konkrétně se jedná jednak o rozšíření jediného funkčního uranového dolu v Rožné na Žďársku, ale i o možné otevření dalších lokalit – v úvahu přichází např. Brzkov a Horní Věžnice na Havlíčkobrodsku, Mečichov na Strakonicku nebo Hamr na Českolipsku.

Uranová těžba by měla být velmi zajímavá nejen z hlediska strategického, ale i ekonomického, neboť cena této komodity na světových trzích neklesá, naopak je možné očekávat její další růst, a to navzdory rozhodnutí Německa a některých dalších zemí o upuštění od získávání energie z jádra. Tento pokles totiž více než vyrovnává velký rozvoj jaderné energetiky v prudce rostoucích ekonomikách „Třetího světa“.

Další potenciálně velmi výnosnou komoditou je zlato, jehož ceny i díky ekonomické nestabilitě vyrostly skutečně raketově. Odhadované české zásoby se přitom pohybují okolo 392 tun, což se podle současných cen rovná více 400 miliardám korun. Možný další cenový nárůst tak nejspíš povede k přehodnocení dosud negativního postoje státních orgánů k těžebním průzkumům zlatonosných nalezišť. Velká ložiska tohoto drahého kovu se nacházejí zejména v Mokrsku na Příbramsku a v Kašperských horách. Kašperské hory ostatně skrývají také ložisko wolframu v hodnotě přes 35 miliard, což je další komodita zmiňovaná v návrhu Surovinové politiky.

Určitého rozvoje se mají podle Strategie dočkat také obnovitelné zdroje energie, jejichž celkový podíl na výrobě elektřiny by měl dosáhnout 15 či více procent. Důraz má být nicméně kladen na ekonomickou efektivitu těchto zdrojů a jejich státní finanční podpora má být postupně omezována. Současný ministr průmyslu a obchodu Martin Kuba je totiž hlasitým kritikem v minulosti prosazované rozsáhlé podpory (především tzv. solárního boomu), který podle něj vedl pouze k zatížení státního rozpočtu a především k rapidnímu růstu cen elektřiny, které v konečném důsledku snižují konkurenceschopnost českých podniků v zahraničí. Takto rozsáhlá podpora byla podle ministra zbytečná a kontraproduktivní ve chvíli, kdy ČR rozhodně nedostatkem elektrické energie netrpí. S důsledky této politiky se bude muset navíc stát vyrovnávat ještě mnoho let. Podpora státu v této oblasti by se tak měla podle dokumentů soustředit spíše na zjednodušení povolovacích procesů či dostupnosti kapacity v síti pro obnovitelné zdroje, než přímé finanční dotace. Hlavním cílem má být zabránění dalšího velkého nárůstu cen elektrické energie.

zdroje: MV, MPO, vlada.cz, prumysl.cz, ČT24, lidovky.cz, novinky.cz

Vybrané události ve sledovaném období

Září

Bezpečnostní cvičení Horizont 2012

Ve dnech 4. – 6. září 2012 proběhlo mezinárodní cvičení složek Integrovaného záchranného systému (IZS) v prostorách elektrické stanice ČEPS, a.s., Nošovice a v blízkosti vedení zvláště vysokého napětí V 404 - Mosty u Jablunkova. Bezpečnostní cvičení, které bylo pracovně nazváno „HORIZONT 2012“, mělo za cíl prověřit krizovou a havarijní připravenost společnosti ČEPS a součinnost jednotlivých složek IZS. Cvičení proběhlo ve spolupráci s provozovatelem slovenské přenosové soustavy SEPS, a.s., Policií ČR, Hasičským záchranným sborem ČR, Armádou ČR, Českým červeným křížem a Policejním sborem Slovenské republiky.
Cvičení HORIZONT 2012 se uskutečnilo pod záštitou ministra vnitra ČR, ministra průmyslu a obchodu ČR a ministerstva hospodářství SR. Ústředním námětem cvičení byl simulovaný útok na významné prvky energetické kritické infrastruktury na území ČR a SR.

Došlo k úspěšnému propojení českého, slovenského a maďarského trhu s elektřinou

Dne 11. září proběhlo propojení trhu s elektřinu tří středoevropských států na principu implicitní alokace přeshraničních kapacit. Tato metoda umožňuje souběžné obchodování na energetických burzách všech tří zemí, až do výše dostupné přenosové kapacity. Propojení trhů by mělo přispět k větší spolehlivosti dodávek, vyšší likviditě trhu a nižší cenové volatilitě. Jedná se o další krok k vytvoření jednotného evropského trhu s elektřinou.

Byly zahájeny práce na komplexní obnově elektrárny Prunéřov 2

Bourací a demoliční práce začaly v polovině září a budou trvat až do března 2013, kdy bude zahájena výstavba tří zmodernizovaných bloků. Ve finále přibude nová strojovna, kotelna, odsiřovací jednotka a další nezbytná zařízení. Akce je součástí širšího programu obnovy uhelných elektráren ČEZ, včetně výstavby nových bloků v hodnotě více než 100 miliard korun. Rekonstrukce Prunéřova 2 navazuje na již skončenou komplexní obnovu elektrárny Tušimice, součástí programu bude také výstavba nových provozů v Ledvicích a Počeradech. Program by měl vést k prodloužení životnosti starších uhelných elektráren a rovněž přispět k jejich efektivnějšímu a ekologičtějšímu provozu.

Po požáru elektrické rozvodny v Trmicích se ocitly bez dodávek tisíce domácností

Požár elektrické rozvodny, ke kterému došlo 19. září v Teplárně Trmice, vyřadil zdroj tepla pro cca 30 000 domácností v Ústí nad Labem a průmyslové odběry. Předběžně určenou příčinou požáru, byla technická závada na zařízení napájecí vody pro kotel K5. Ke zranění osob nedošlo. Dodávky byly kompletně obnoveny v řádu dní.

Říjen

Ze soutěže o dostavbu Temelína vypadla francouzská Areva

ČEZ byl nucen vyřadit nabídku společnosti Areva z dalšího posouzení a hodnocení soutěže na dostavbu bloků 3 a 4 jaderné elektrárny Temelín, a to z důvodu zásadních nedostatků a nesplnění předem vylučujících kritérií jak obchodních, tak i zákonných. Neúspěšný uchazeč následně podal odvolání vůči tomuto rozhodnutí na Úřad pro ochranu hospodářské soutěže, což

vedlo k částečnému přerušení posuzování zbývajících dvou nabídek. V prosinci ČEZ nicméně oznámil, že předběžné hodnocení nabídek ukončí na konci února. Do září by tak měl být znám vítěz celého tendru a do konce příštího roku by měla být podepsána smlouva s vítězem. Ve hře tak zůstávají dvě nabídky – česko-ruského konsorcia MIR.1200 a americké firmy Westinghouse.

Výsledky zátěžových testů evropských jaderných elektráren
V říjnu zveřejnila Evropská unie výsledky zátěžových testů evropských jaderných elektráren. Kontroloři poukázali na několik stovek nedostatků, zároveň ovšem konstatovali, že žádná jaderná elektrárna v EU není v tak špatném bezpečnostním stavu, aby ji bylo nutné okamžitě zavřít. Bude ale nutné do jejich bezpečnosti dále výrazně investovat. Tyto investice se nevyhnou ani oběma českým elektrárnám – Dukovany a Temelín by mohlo, podle některých odhadů, vylepšení zabezpečení přijít dohromady až na 1,5 miliardy korun. Veškerá opatření mají být dokončena do konce roku 2015. K zátěžovým testům přistoupila EU po incidentu ve Fukušimě, odhady na nutné investice na jejich základě se pohybují od 10 – 25 miliard eur.

Rusko otevřelo druhou větev plynovodu North Stream
Kapacita přepravy se tímto krokem zdvojnásobuje na 55 miliard metrů krychlových, což představuje zhruba třetinu současného vývozu Gazpromu do Evropy. Kvůli slabé poptávce však objem přepravy zatím zůstává beze změn, kapacita první větve byla naplněna z pouhých 34 procent. Hlavním důvodem pro vybudování North Streamu byla snaha Ruska a Německa vyhnout se tranzitu přes „problémové země“, tedy především Ukrajinu a Bělorusko. Na North Stream navazují další plynovody, které ruský plyn rozvádějí dál do EU. Jedná se především o Opal, který vede do Saska a na něj navazující Gazelu, která je před dokončením a má zásobovat Česko a jižní Německo.

Listopad

Výbuch plynu v koksovně ArcelorMittal v Ostravě
Při výbuchu na plynovém hospodářství koksárenské baterie č. 11 bylo 7. listopadu zraněno celkem 9 lidí, včetně čtyř členů indické delegace, která bylo v podniku na technické návštěvě. Jeden z Indů později v nemocnici zemřel.
Dosud není zcela jasné, co tuto nehodu způsobilo. V 10:15 došlo ke vznícení plynu, který unikl při technologické manipulaci. Podle mluvčí společnosti ArcelorMittal nedošlo při incidentu k úniku žádných škodlivých látek. Policie případ zatím vyšetřuje jako trestný čin obecného ohrožení z nedbalosti.

Vláda vzala na vědomí návrh státní energetické koncepce
8. listopadu byla na zasedání Vlády ČR projednáván návrh státní energetické koncepce. Ministři jej vzali na vědomí, před konečným schválením si nicméně Vláda vyžádala posouzení dopadů naplňování tohoto dokumentu na životní prostředí. Státní energetická koncepce je zásadním strategickým materiálem v oblasti energetické bezpečnosti. Současné znění návrhu vyvolalo množství negativních ohlasů zejména mezi ekologickými organizacemi.

Společnost ČEPS udělila medaile zástupcům bezpečnostní komunity
Dne 30. listopadu došlo v prostorách Míčovny Pražského hradu ke slavnostnímu předání 21 „medailí za bezpečnost“, kterými společnost ČEPS ocenila spolupráci s pracovníky orgánů veřejné správy a samosprávy a s příslušníky složek Integrovaného záchranného systému, zejména Policie ČR, Hasičského záchranného sboru ČR, Armády ČR, kteří se významně zasloužili o úspěšné plnění úkolů a závazků společnosti ČEPS v oblasti ochrany kritické infrastruktury.

Největší větrná farma v Evropě zahájila zkušební provoz

Dne 22. listopadu byla do sítě připojena poslední z 240 turbín větrného parku Fantanele a Cogealac v Rumunsku, nedaleko Černého moře. Celkový výkon této farmy je 600 MW a může zásobovat elektřinou přes milion domácností, což z ní činí největší pevninský větrný park Evropy. Investorem projektu je česká společnost ČEZ, která jej označuje i za jeden z nejvýznamnějších počinů v oblasti obnovitelné energie ve světě. Skupina ČEZ hodlá zkušeností z Rumunska využít také v Polsku, kde plánuje v rámci projektu Eco-Wind spustit větrné elektrárny o celkovém výkonu zhruba 700 MW.

Česko získalo podíl v ropovodu TAL

Za nikoliv nevýznamné posílení české energetické bezpečnosti je možné označit zisk pětiprocentního podílu v ropovodu TAL od společnosti Shell Deutschland, ke kterému došlo prostřednictvím státem vlastněného přepravce ropy MERO. V praxi to totiž znamená, že ČR už nebude tolik závislá na dodávkách ropovodem Družba, kterým proudí ropa z Ruska. Akcionáři s minimálně pětiprocentním podílem mají totiž nejen právo nominovat svého zástupce do řídícího výboru společnosti, ale především mají přednostní právo transportu své ropy. Mimo jiné by to mohlo znamenat také přístup k lepším cenám za přepravu ropy z Terstu a teoreticky by Česko mohlo přes ropovod IKL v případě potřeby zásobovat i další státy, například Slovensko či Maďarsko.

Ropovod TAL začíná v italském Terstu a vede do Německa. Proudí jím ropa z kaspické oblasti, především z Ázerbájdžánu, Blízkého východu a severní Afriky. Největším podílníkem je rakouská ÖMV. Ropovod Družba se potýká s častými technickými závadami, problémy mu způsobují i občasné špatné klimatické podmínky na Sibiři. Důvody k přerušení dodávek z Ruska ale mohou mít i politický podtext.

Prosinec

ČEZ prodává svou albánskou distribuční společnost

V prosinci nabídl ČEZ k prodeji svou distribuční společnost v Albánii CEZ Shpërndarje. K tomuto kroku sáhl po sérii problémů a sporů s albánskou vládou. Společnost ČEZ vstoupila na albánský trh v květnu 2009 nabytím 76% podílu v albánské distribuční společnosti, jejímž čtvrtinovým vlastníkem zůstal albánský stát. Nákup byl součástí širší strategické expanze ČEZu do oblasti jihovýchodní Evropy.

V roce 2012 se nicméně jeho působení v zemi začalo komplikovat, kdy v důsledku katastrofálního sucha zvýšil státní výrobce elektřiny KESH výkupní ceny dceřinné společnosti ČEZu, ta však nesměla toto navýšení promítnout do koncových cen pro zákazníky. Vše vyvrcholilo přerušením dodávek do albánských vodáren, po kterém albánský regulátor zahájil proces odebrání licence. ČEZ se nakonec rozhodl se své ztrátové albánské společnosti zbavit, celá investice tak bude pro firmu zřejmě značně ztrátová. Skupina ČEZ zahájila kroky k uplatnění záruky Světové banky.

Stát nesníží příspěvek na obnovitelné zdroje

Třebaže podle původních plánů mělo být na podporu obnovitelných zdrojů vyčleněno jen 9,7 miliardy korun, vláda se rozhodla zachovat současnou výši příspěvku, tedy 11,7 miliard korun. Dotací ze státního rozpočtu se vláda snaží zabránit růstu cen elektrické energie, který by mohl snížit konkurenceschopnost českých firem a vést k propouštění. Ministr Martin Kuba v této souvislosti připomněl, že stát stále doplácí na nešťastně nastavenou legislativu z času velkého boomu solárních elektráren, který započal v roce 2010. Tuto energii přitom podle ministra ČR nepotřebuje, protože má elektřiny v současné době nadbytek. Konečné rozhodnutí o poplatku spotřebitelů ale vynese až Energetický regulační úřad.

BEZPEČNOST FINANČNÍCH INSTITUCÍ

Policejní statistiky a jejich interpretace

Trestné činy za období 1. 1. – 30. 9. 2012 dle „druhu napadených objektů“

druh objektu	zjištěno tr. činů	škody
spořitelny	71	2 569 200 Kč
pojišťovny	96	4 073 800 Kč
banky	170	13 465 900 Kč
směnárny	12	1 335 700 Kč
spořitelní a úvěrová družstva	4	222 500 Kč
celkový součet[4]	**353**	**21 667 100 Kč**

První prezentovanou statistikou jsou opět data podle druhu napadených objektů. Z nich lze vyčíst, že v prvních třech čtvrtinách roku bylo v souvislosti s finančními institucemi evidováno celkem 353 trestných činů a napáchané škody přesáhly 20 milionů korun. Také v tomto případě je nicméně nutné se na statistiky podívat podrobněji a správně je interpretovat.

Naprostou většinu uvedených trestných činů tvoří krádeže prosté, krádeže vloupáním a různé formy podvodů. Do statistik se přitom dostanou všechny ty krádeže, ve které hrála finanční instituce roli napadeného objektu. Zdaleka se přitom nemusí jednat jen o přepadení pobočky, ale může jít například o vloupání do služebního vozu nějaké bankovní instituce. To lze demonstrovat na konkrétním příkladě: v případě bank mělo celkem 38 (z celkového počtu 172) evidovaných trestných činů souvislost s motorovými vozidly (jejich odcizení, vykradení, poškození atd.). Celková škoda z těchto skutků přesáhla 2 miliony korun.

Kromě krádeží způsobily největší celkové škody nejrůznější podvody. V případě všech uvedených finančních institucí se jednalo celkem o 34 případů podvodu, což je sice jen asi desetina z celkového počtu trestných činů, celkové škody zde nicméně přesáhly 7,5 milionu korun (což je zhruba třetina celkové výše škod).

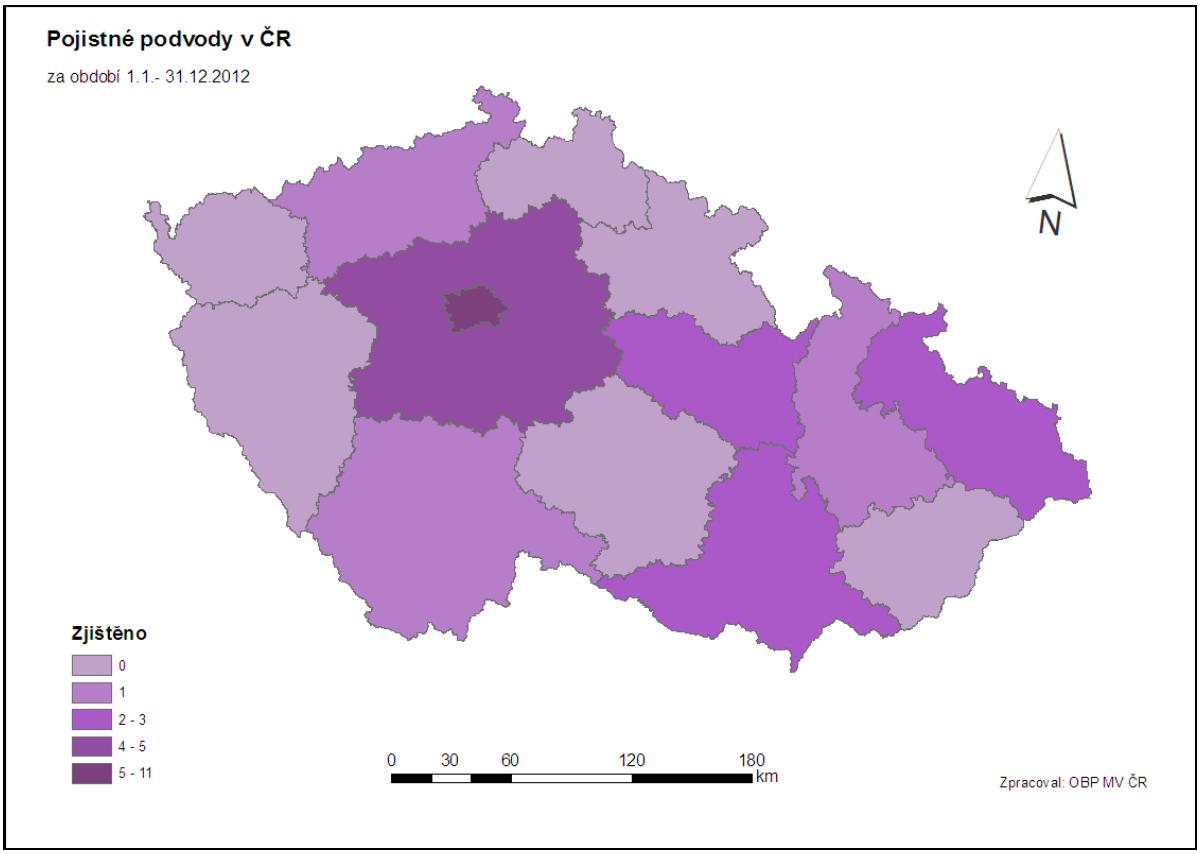
Z těchto čísel je jasně viditelné určité zkreslení, které výše uvedená statistika podle druhu napadených objektů představuje. Skutečné škody za podvodná jednání jsou totiž mnohem vyšší, ne vždy je ale finanční instituce v policejní zprávě explicitně zmíněna jako napadený objekt. Pro získání komplexnějšího obrazu je proto vhodné dopomoci si dalšími statistickými daty, např. využitím údajů o počtu trestných činů členěných podle paragrafů trestního zákoníku.

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

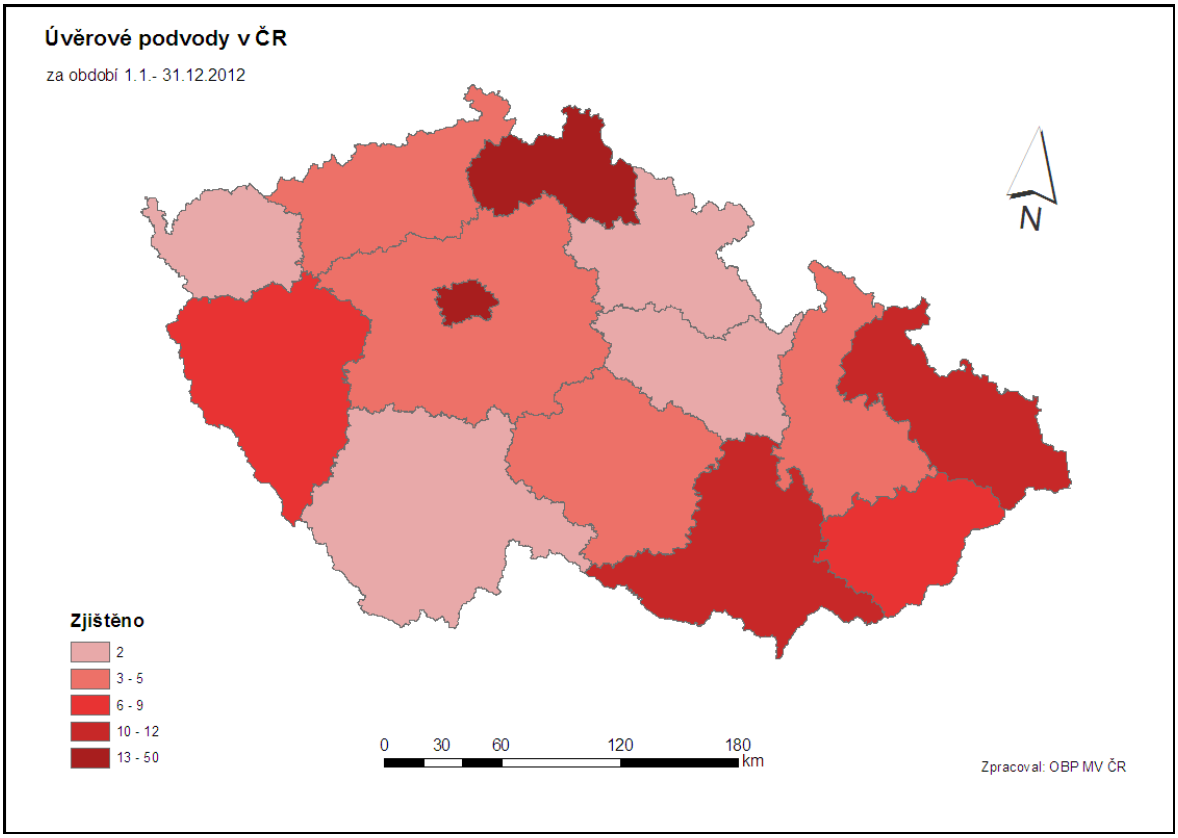
Z pohledu finančních institucí jsou zajímavé především údaje o §210 a 211 trestního zákoníku, tedy pojistné a úvěrové podvody. Hlavní údaje týkající se těchto dvou typů trestných činů v průběhu celého uplynulého roku shrnuje následující tabulka:

typ trestné činnosti	zjištěno	objasněno	stíháno osob	celková výše škod
pojistné podvody	26	18	19	82 696 000 Kč
úvěrové podvody	165	146	154	773 050 000 Kč

Vidíme, že v tomto případě se již škody pohybují v částkách desítek milionů korun, u úvěrových podvodů se dokonce šplhají až nad tři čtvrtě miliardy. **Pozitivní zprávou je naopak fakt, že objasněnost těchto (zjištěných) trestných činů ze strany policie je poměrně vysoká** – v případě úvěrových podvodů činí více než 88%, u podvodů pojistných se pohybovala okolo 70%. Pro úplnost připojujeme dvě mapy, na kterých je znázorněna incidence výskytu tohoto typu trestných činů v rámci České republiky.



Jak je zřejmé i z mapy na následující straně, k podvodnému jednání celkem logicky dochází nejčastěji ve velkých městech (a tedy i krajích s největšími metropolemi). Některé kraje ovšem do tohoto jednoduchého schématu úplně nezapadají. Např. v počtu úvěrových podvodů předstihl Liberecký kraj i mnohem lidnatější kraje (např. Ústecký, Olomoucký) a naopak kupříkladu kraj Pardubický stojí mimo svou očekávatelnou pozici v počtu podvodů pojistných.



Mezi dalšími evidovanými protiprávními činy lze uvést například vydírání, poškozování cizí věci, zatajení věci, sprejerství atd. Pro konkrétnější údaje z velmi sledovaných případů loupeží na finančních institucích můžeme sáhnout do jiné policejní statistiky, kde máme v tomto případě k dispozici data téměř za celý rok (od 1. 1. do 30. 11. 2012). Údaje shrnuje následující tabulka:

Loupeže na finančních institucích za období 1. 1. – 30. 11. 2012

zjištěno	z toho ukončeno prověřování	objasněno	celková výše škod	zajištěno policií
125	104	69 (55%)	8 911 000 Kč	2 071 000 Kč

Z uvedených statistik vidíme, že v celé České republice došlo v uplynulém roce (přesněji v jeho podstatné části) k více než stovce loupeží na bankovních institucích, přičemž pachatelé si odnesli téměř 9 milionů korun. Dva miliony korun se policii následně podařilo zadržet. Zhruba u poloviny případů byl nalezen pachatel.

Celkem bylo za tato loupežná přepadení stíháno 41 osob, z toho jen jedna žena. Polovinu stíhaných tvořili recidivisté, žádný pachatel nebyl mladší než 18 let. Vzhledem k tomu, že bankovní loupeže jsou velmi medializovaným tématem, může být snadné podlehnout dojmu, že jejich počet neustále narůstá. Opak je ale na řadě míst pravdou.

Například v Praze se celkový počet loupežných přepadení postupně snižuje. Konkrétně u bank klesl celkový počet přepadení od roku 2007 zhruba na třetinu. V roce 2012 se počet těchto incidentů pohyboval okolo dvaceti (nejsou k dispozici data za prosinec), ještě před pěti lety to přitom bylo v průměru 60 loupeží ročně. Klesají rovněž škody, které pachatelé při těchto akcích finančním institucím způsobují. Zatímco před čtyřmi lety si pachatel z jedné krádeže odnesl v průměru čtvrt milionu korun, dnes je to průměrně jen 75 tisíc.

V mnoha případech se jedná o amatérské zloděje, které policie snadno dopadá krátce po samotném činu. Médii proběhly kuriózní až komické případy z minulého roku, kdy například zloděj při odchodu z banky ztratil zbraň i lup. Při jiném pokusu si zase pokladní vůbec nevšimla, že se jedná o přepadení, protože pachatel držel zbraň tak nešikovně, že ji nemohla vidět. Když nějakou dobu na jeho přítomnost nereagovala, muž zklamaně odešel. Amatérismus je ve skutečnosti v případě bankovních loupeží spíše pravidlem, než výjimkou. Většinou se jedná o skutky jednotlivců, kteří se pokoušejí přijít snadno k penězům, **organizované gangy v České republice v současné době nepůsobí** (v minulosti se ale takové případy vyskytly).

Přesto pochopitelně dochází i k situacím, kdy se pachateli daří policii unikat i přes celou sérii úspěšných loupeží. Více než rok například stále uniká pachatel (pravděpodobně se jedná o slovenského občana), který má na svědomí množství úspěšně vyloupených bank hned v několika státech – České republice, Slovensku i Rakousku. Nedaří se jej dopadnou navzdory tomu, že po něm intenzivně pátrají policejní sbory tří zemí a Interpol. Případy opakovaných neodhalených přepadení jsou ale čím dál vzácnější.

Platební karty a bankomaty

Podle údajů pražské policie nepůsobila v hlavním městě v minulém roce ani jediná organizovaná skupina, která by se soustředila na loupežná přepadení, což je fakt, který nám může řada světových metropolí závidět. 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 výdělku i náklady na provedení jsou u těchto novějších typů kriminality výrazně nižší. Tomuto fenoménu se blíže věnuje následující kapitola o kyberbezpečnosti.

Rapidní nárůst lze zaznamenat zejména v případě skimmingu a dalších forem zneužití bankomatů a platebních karet. České banky sice například věnují miliony korun na ochranu svých bankomatů, zloději ale znovu a znovu přicházejí s vylepšeními, které tato bezpečnostní opatření překonávají. Již v průběhu března 2012 tak policie zaznamenala stejné množství případů pokusů o zneužití dat z platebních karet, jako v celém roce 2011. Počátkem roku byl například zadržet dvoučlenný gang, kterému se podařilo díky skimmingu získat kopie více než šesti set kreditních karet.

Vyrobit si skimmovací zařízení či vlastní kreditní kartu je totiž překvapivě snadné. Na internetu jsou všechny součásti běžně dostupné, a to např. včetně klávesnic a dalších součástí bankomatů, které prodávají čínské firmy jakožto „náhradní díly“. Nákup takových zařízení je přitom zcela legální. Podle některých bezpečnostních expertů nicméně banky stále nedělají pro zabezpečení karet a bankomatů maximum. Ukradené částky se totiž stále pohybují jen v milionech, náklady na bezpečnostní opatření pak v miliardách, takže se bankám vyplatí spíše vyplácet náhrady okradeným klientům.

Určité nebezpečí představují také koncová platební zařízení, například pokladní čtečky kreditních a debetních karet. Tato zařízení přitahují kyberzločince především tím, že data z platebních karet jsou zde shromažďována v daleko kompletnější podobě. Při získání těchto údajů není problém vyrobit si vlastní kopii karty včetně funkčního magnetického pásku.

Rizikové jsou zejména malé obchody, které často nedodržují nejnovější bezpečnostní standardy a normy, jako je například PCI-DSS, která povinně využívá šifrování a zakazuje uchovávání dat z magnetických pásků na terminálech. V Evropě a USA se počet nezabezpečených čteček postupně snižuje, např. v zemích Latinské Ameriky či v Asii je jich ale stále velmi mnoho a po platbě kartou v obchodě tak mohou být ohroženi i čeští turisté. Malware zaměřený na zneužití čteček je přitom stále sofistikovanější, nejnovější z nich dokáží prolomit i poměrně pokročilé šifrování, což vytváří tlak k neustálé aktualizaci bezpečnostních norem.

Riziko v kyberprostoru

Stále častější jsou také hackerské a phishingové útoky, které jsou velkou hrozbou pro celé odvětví internetového bankovnictví. Banky pak musejí v reakci na ně sahat k mimořádným opatřením jako jsou blokace těchto služeb nebo dokonce platebních karet, což je pro jejich zákazníky nepříjemné a způsobuje to další finanční ztráty.

Jedním z nejsledovanějších případů uplynulého roku byl virus Eurograbber, kterému se podařilo zneužít desítky tisíc účtů po celé Evropě. Šlo o nejrozsáhlejší útok tohoto typu v evropské historii a částečně jej lze připsat na vrub rozšíření „chytrých“ telefonů. Staré telefony bez přístupu k internetu totiž nebylo možné zavirovat, ochrana plateb skrze autorizaci SMS byla tudíž podstatně spolehlivější.

Ohroženy jsou zejména malé a střední firmy, které často nevynakládají velké prostředky na vlastní zabezpečení. **Průzkum Ponemon Institute v USA ukázal, že ze zkoumaných více než 500 podniků s méně než 200 zaměstnanci, se jich 56% stalo cílem útoku na bankovní účet.** 78% podvodných převodů přitom bylo zjištěno až poté, co peníze zmizely. Odpovědnost firem a bank za bezpečnost platebních převodů je přitom sdílená – banky mají k odhalování podvodů mnohem lepší know-how i technické prostředky, je pro ně ovšem mnohem těžší identifikovat podezřelý převod. Firmy by tak neměly zanedbávat investice do vlastního zabezpečení. Někteří experti dokonce doporučují, aby si každá společnost vyhradila jeden počítač výhradně pro internetové bankovnictví, což je ovšem zejména v malých firmách obtížně proveditelné.

Vybrané události ve sledovaném období

Září

Phishingové útoky na klienty České spořitelny

V září 2012 vydala Česká spořitelna varování před podvodnými e-maily, které se pokoušely z klientů této banky vylákat údaje o kreditní kartě. Tyto zprávy se snažily vzbudit dojem, že se jedná o oficiální komunikaci ČS se svými zákazníky a většinou oznamovaly přechod na nový systém zabezpečení, případně upozorňovaly na údajné pochybné transakce na příjemcově účtu. Následně požadovaly zaslání všech údajů, nutných pro internetovou platbu platební kartou. Podle podvodníků, vydávajících se za zaměstnance banky, byly totiž tyto údaje nutné pro aktivaci lepšího zabezpečení, případně pro autorizaci účtu a platební karty, jimž v případě nezaslání hrozí zablokování.


ČESKÁ SPOŘITELNA

Vážený klient/Klientko,

Jelikož vyvíjíme služby naší banky, tzn. osobní účet v České spořitelně, ke kterému máte aktivovanou debetní kreditní kartu VISA a v poslední době jsme zaznamenali na Vašem účtu podezřelé platební transakce, je potřeba aktualizovat data Vaší kreditní karty , v opačném případě bude Vaše kreditní karta zablokovaná a Váš účet pozastaven na dobu neurčitou. Chceme pouze ověřit, že transakce na Vašem účtě oprávněn provádíte/ky, jako disponent účtu a ne někdo jiný.

Pošlete nám prosím níže vyplněné parametry:

Jméno a příjmení: _____

Rodné číslo: _____/_____

Bydliště: _____

Tel.číslo: _____

Číslo kreditní karty: _____

Platnost karty od a do: _____

CVC kód (poslední 3 čísla na zadní straně): ____

Vložka zaměstnance:

Bankéř klientského centra
Pro rychlejší platební kart

Bezpečnost při platbách kartou

Česká spořitelna a.s.

S pozdravem

Bankéř klientského centra

Česká spořitelna, a.s., Praha 4 Olbrachtova 1929/62 PSČ 140 00, IČ: 45 24 47 82
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 1171

Jednalo se o ukázkový příklad phishingu a zároveň o potvrzení stále větší rafinovanosti tohoto typu podvodu i v českém prostředí. Dříve byly tyto útoky mnohdy prováděny ze zahraničí a byly napsány velmi špatnou češtinou, většinou prací automatického překladače. Novější e-maily ovšem působí mnohem profesionálnějším dojmem – některé verze byly opatřeny originálním logem a grafikou ČS a dokonce i fotografií skutečné zaměstnankyně banky. Celkový objem finančních prostředků, které se podařilo touto cestou z podvedených lidí vylákat, není v tuto chvíli znám. Podobné emaily se později objevily i v případě dalších finančních institucí, např. ČSOB.

Ozbrojený muž vyloupil banku v Plzni a byl zadržen policií

13. září došlo na Americké třídě v Plzni k bankovnímu přepadení. Padesátiletý Slovák si z banky pod pohrůžkou použití střelné zbraně odnesl 10 tisíc korun. Záhy jej ale při jízdě směrem na Prahu zadrželi policisté. Policie v současné době vyšetřuje, zda se tento muž nedopustil i dalších loupeží.

Reiffeisenbank zablokovala svým klientům kvůli hackerům platby přes internet

Vzhledem k tomu, že se hackerům podařilo získat údaje o platebních kartách z několika zahraničních internetových obchodů, přistoupila Reiffeisenbank v září k mimořádnému kroku a zablokovala všem svým klientům veškeré internetové platby. Banka také již zaznamenala několik desítek pokusů o zneužití ukradených dat.

Pokud si klienti této banky v dané době přáli zaplatit kartou on-line, museli si danou službu sami odblokovat. Banka nicméně doporučovala, aby ji po úspěšně provedené platbě okamžitě zase zablokovali. Upozornila na případ jednoho ze zákazníků, kterému byly v řádu hodin po odblokování z karty odcizeny finanční prostředky. Banka v tomto případě vyplácí klientům ukradené peníze zpět a navíc nabídla zdarma speciální virtuální kartu, se kterou lze na webu platit.

Česká národní banka vydala varování před aktivitami Paramount Financial Group

V září zveřejnila Česká národní banka na svých stránkách upozornění, že společnost Paramount Financial Group se sídlem ve Vídni nemá v současné době oprávnění k poskytování investičních služeb na českém finančním trhu a není ze strany ČNB dohlížena. Tato společnost přitom oslovuje telefonicky v anglickém jazyce i potenciální české investory. Před touto firmou navíc varuje i norský dohledový orgán Finanstilsynet. Obdobné varování vydala ČNB ve sledovaném období také před kyperskou společností Zoompartners Ltd. a firmou Golden Grail Ltd. se sídlem na Seychelách (s pobočkou v Brně v Holandské ulici).

Říjen

Policii se podařilo zadržet v Dominikánské republice gang, který v ČR přepadával a okrádal banky

Výrazný úspěch, který mj. zvýšil prestiž České republiky v organizaci Interpol, zaznamenala česká policie. V rámci akce Dominik se jí podařilo zadržet celkem 8 osob, které byly v České republice hledány pro závažnou trestnou činnost, včetně rozsáhlých bankovních podvodů a přepadení finančních institucí. ČR nemá s Dominikánskou republikou uzavřenu dohodu o vydávání osob, proto se v této zemi ukrývá řada českých zločinců. Díky spolupráci s Interpolem a místní policií se nicméně daří jejich zadržování. Již v červenci byl v této zemi zatčen František Hajn, který se zřejmě podílel na známém přepadení vozu bezpečnostní agentury, při které bylo odcizeno více než 154 milionů korun. Počet zadržených při akci Dominik mohl být ještě větší, celou operaci totiž neplánovaně zkomplikoval hurikán Sandy, který znemožnil přístup do některých oblastí.

Platby přes internet pouze po autorizaci přes SMS

Od 1. října 2012 musí všichni klienti ČSOB potvrdit každou platbu kartou přes internet prostřednictvím kódu, který jim přijde na mobilní telefon. ČSOB k tomuto kroku přistoupila vzhledem k rostoucímu počtu hackerských útoků, které se pokoušejí získat údaje o platebních kartách a následně je zneužít k převodu finančních prostředků (viz případ Reiffeisenbank ze září 2012). Není tak první a zřejmě ani poslední bankou, která toto bezpečnostní opatření zavádí.
S problémem zneužití karet svých zákazníků se potýká celá řada bank. V červnu 2011 například hackeři ukradli údaje o několika stovkách tisíc platebních karet společnosti Citigroup. Častější jsou ale hackerské útoky na zahraniční internetové obchody, jejichž zabezpečení proti kybernetickým útokům je mnohdy horší, než u těch tuzemských. Druhou možností je vylákání údajů ze samotných zákazníků, buď prostřednictvím phishingových útoků, počítačových virů, či formou skimmingu v bankomatech (posledně jmenovaný problém ovšem zavádění SMS autorizace platby neřeší).

Dopaden recidivista, který dvakrát za sebou přepadl banku v Brně

Pobočka České spořitelny v brněnské Křídlovické ulici patří mezi nejčastěji přepadávané banky v Česku. V červenci a znovu 18. září 2012 zde dvakrát loupil stejný pachatel, mnohonásobně (celkem 22x) trestaný recidivista, který si odnesl celkem několik set tisíc korun. Díky kvalitní práci policie se jej podařilo v říjnu zadržet blízko kojeneckého ústavu, kam chodil pravidelně navštěvovat své děti. Hrozí mu až deset let vězení.
V Brně evidovali policisté za rok 2011 360 loupežných přepadení, v průměru tedy téměř jedno denně. Kromě bank jsou nejčastějším terčem herny a sázkové kanceláře. Objasněnost těchto případů se pohybuje kolem 55%.

Neúspěšný pokus o vyloupení banky s granátem v ruce

3. října došlo k pokusu o vyloupení banky v Horní ulici v Havlíčkově Brodě. Muži s granátem se podařilo získat od pracovníků banky finanční hotovost, při odchodu byl ale zadržen civilní osobou a předán policii. Granát byl přitom skutečný a po zatčení pachatele vyšlo najevo, že měl u sebe navíc ještě krátkou střelnou zbraň.

Listopad

Výuka finanční gramotnosti na základních školách

V listopadu oznámilo ministerstvo školství svůj plán na úpravu rámcových vzdělávacích programů. Od příštího roku by měly školní osnovy více akcentovat například výuku o korupci či finanční gramotnost. Je na samotných školách, jakým způsobem si tyto zapracují do svých

vzdělávacích programů – zda pro novinky vytvoří samostatný předmět, nebo jejich výklad zařadí do těch stávajících např. do občanské nauky či matematiky.
Řadu rodin dnes trápí nedostatečná orientace ve finančních produktech a neschopnost hospodaření v časech krize. Odborníci proto upozorňovali, že dětem je třeba vštěpovat základní dovednosti nakládání s penězi už od školních lavic. Jedná se o vysoce praktické téma, které navíc děti baví víc, než např. abstraktní výpočty v matematice, a tudíž jej lze využít i pro zpestření a zpříjemnění výuky klasických předmětů.

V Praze byla otevřena první vietnamská banka
Druhý největší finanční ústav ve Vietnamu, Vietnamská investiční a rozvojová banka, otevřela v listopadu v Česku své zastoupení. Cílí tak především na početnou vietnamskou komunitu, která tento krok velmi vítá. Vietnamští obchodníci a živnostníci často naráželi v českých bankách na jazykovou bariéru a „nepřístupnost“, jak uvedl jeden z nich. Kromě Vietnamců žijících v ČR chce banka oslovit také české firmy podnikající na asijském trhu. Vietnamská komunita, třetí nejpočetnější skupina cizinců v Česku, tak má již kromě vlastního televizního kanálu či školek nově k dispozici také vlastní finanční ústav.

Prosinec

Reiffeisenbank preventivně zablokovala na 3 tisíce platebních karet
Poté co již v září zablokovala Reiffeisenbank všem svým klientům dočasně platby přes internet, přistoupila tato banka v prosinci k dalšímu mimořádnému bezpečnostnímu opatření. U třech tisícovek svých klientů provedla blokaci jejich kreditních karet, které si postižení lidé musí nechat vyměnit. Důvodem byla ztráta údajů u firmy, zprostředkovávající bezhotovostní platby u zahraničních obchodníků. Opatření se tak netýkalo jen Čechů, ale řady karet používaných ve střední a východní Evropě, resp. všech těch, se kterými klienti zaplatili u konkrétního obchodníka. Ke zcizování dat přitom údajně docházelo již od července, odhaleno bylo ale až nyní. O peníze prý nikdo z českých zákazníků nepřišel. Banka informovala své klienty o události prostřednictvím SMS a následně je vyzvala k výměně karty.

Viru Eurograbber se podařilo obejít autorizační SMS a hackeři tak ukradli téměř miliardu korun
Mobilní textová zpráva s kódem, který autorizuje internetovou platbu, bývá považována za velmi spolehlivé bezpečnostní opatření. Některé české banky jej tak zavádějí i pro on-line platby kartou. Jak ale ukazuje poslední případ rozsáhlé kybernetické krádeže, ani tento způsob ochrany není stoprocentně účinný a hackeři již našli způsob, jak jej obejít. Mohou za to především chytré telefony.
Viru Eurograbber se podařilo nabourat internetové bankovnictví u 30 tisíc lidí z 32 různých bank z celé Evropy a odcizit celkem 36 milionů eur (přes 900 milionů korun). Největší škody zaznamenaly banky v Německu, Itálii, Španělsku a Holandsku, v tuto chvíli není jasné, zda jsou mezi postiženými i lidé z Česka. Šlo o mimořádně dobře připravený a sofistikovaný útok, při kterém se hackerům podařilo získat kontrolu jak nad počítačem, tak nad mobilním telefonem klienta.
Eurograbber se šířil jako klasický počítačový virus, který po přihlášení do internetového bankovnictví odeslal hackerům údaje o účtu i telefonní číslo klienta. Tomu pak na jeho mobil přišla podvodná phishingová zpráva, která se vydávala za informaci od banky. Vyzývala k nainstalování aktualizované aplikace pro přístup k internetovému bankovnictví. Této zprávě uvěřily desítky tisíc lidí a hackeři tak ovládli jak jejich počítače, tak jejich mobily. Zneužití peněz na účtu bylo pak již snadné.

INFORMAČNÍ TECHNOLOGIE A KYBERNETICKÁ BEZPEČNOST

Policejní statistiky a jejich interpretace

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

Informační kriminalitou rozumíme takovou trestnou činnost, která je páchána v prostředí informačních technologií, kdy předmětem útoku je buď samotná oblast informačních technologií, případně je tato trestná činnost prováděna za výrazného využití informačních technologií.

Termín informační kriminalita (IK) je tedy označením pro poměrně širokou skupinu trestných činů, které spojuje určitý společný faktor, daný právě formou páchání tohoto typu trestné činnosti. Jedná se většinou o následující typy trestné činnosti: porušování autorských práv, různé podvodné aktivity, krádeže elektronických dat, útoky zaměřené na destabilizaci datových sítí, šíření závadného elektronického obsahu (dětská pornografie, extremistická ideologie), ale také o vydírání, vyhrožování a poměrně nově i o tzv. stalking (nebezpečné pronásledování).

Určit přesný rozsah informační kriminality páchané na území České republiky je velmi obtížné. Klasické policejní statistiky dle druhu napadeného objektu, které jsme prezentovali v předchozích dvou kapitolách, jsou v tomto případě jen velmi stěží využitelné:

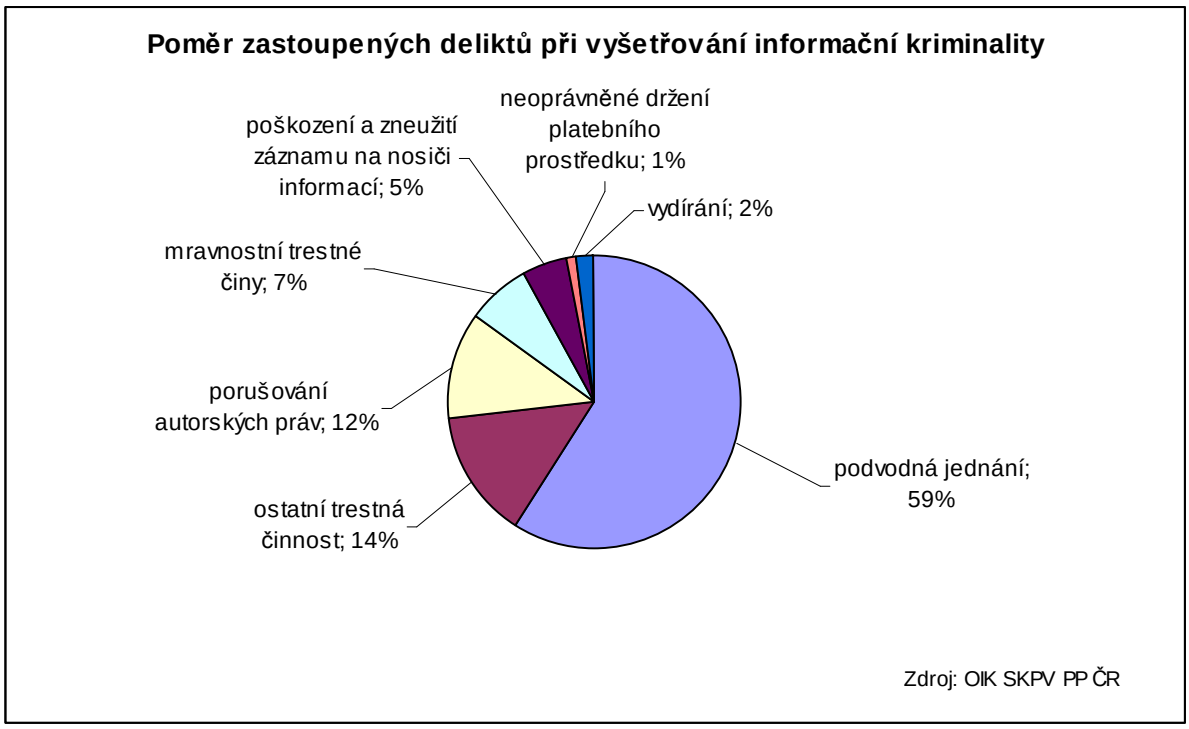
Trestné činy za období 1. 1. – 30. 9. 2012 dle „druhu napadených objektů“

druh objektu	zjištěno tr. činů	škody
internet	7	106 600 Kč
datová síť	3	217 400 Kč
celkový součet	**10**	**324 000 Kč**

V této statistice je pochopitelně evidován jen nepatrný zlomek skutečného objemu kybernetické kriminality v ČR. Zahrnuty jsou zde jen ty případy trestných činů, při který policista při vyplňování příslušného protokolu přímo označil internet či datovou síť za napadený objekt. Obvyklejší přitom je, že je do formuláře zapsána konkrétní postižená osoba či firma.

Pro konkrétnější statistické údaje se tedy musíme obrátit na přímo na specializované policejní pracoviště. V současné době je problematika IK řešena v rámci Policie ČR v oblasti výkonné složky na centrální úrovni Odborem informační kriminality Úřadu služby kriminální policie a vyšetřování Policejního prezidia ČR. Toto pracoviště zpracuje v oblasti elektronických podání a poznatků zhruba 1033 případů ročně, v dalších stovkách případů pak poskytuje odbornou podporu jiným policejním složkám.

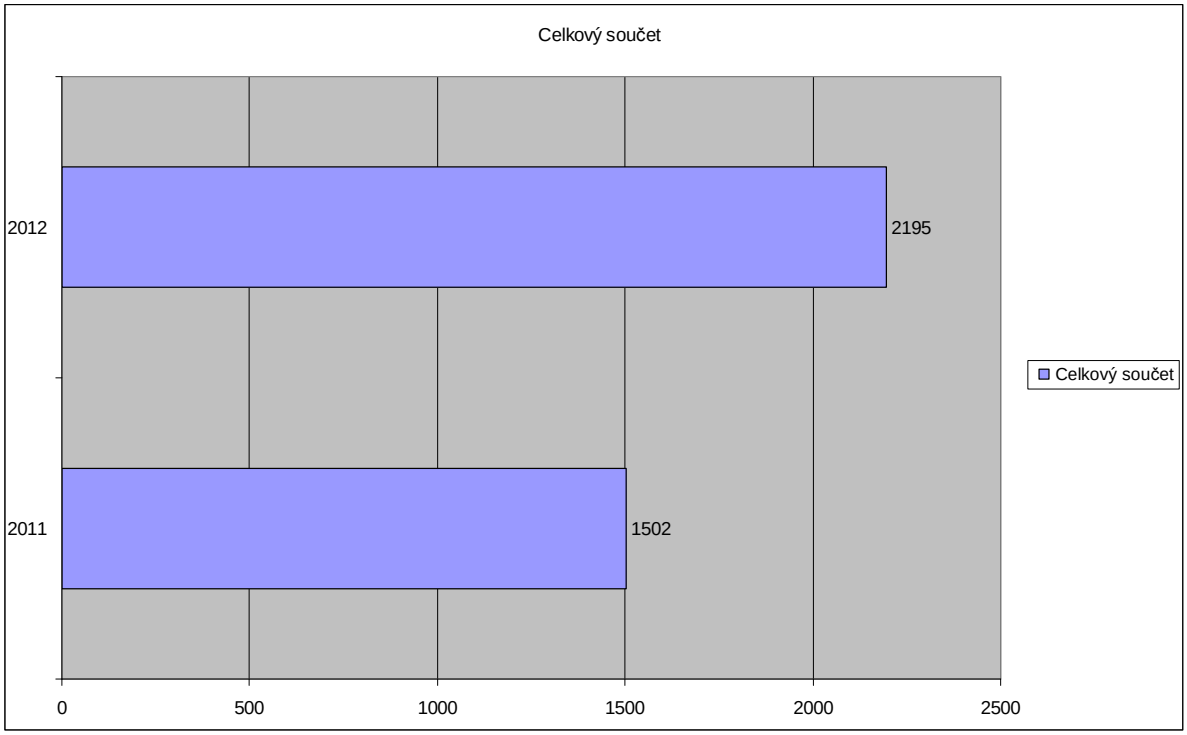
V současné době jsou nejčastěji řešeným typem trestné činnosti různé formy podvodného jednání, které dnes tvoří 59% všech deliktů řešených při vyšetřování informační kriminality. V trojici nejčastěji řešených forem IK následuje porušování autorských práv (12%) a mravnostní trestné činy (7%). Je nutné říci, že v případě IK se jedná o velmi dynamickou oblast trestné činnosti, ve které policisté neustále narážejí na zcela nové a originální formy nezákonného jednání. Velkým problémem je také značná mezinárodní provázanost informační kriminality, kdy její účinné potírání mnohdy vyžaduje úzkou součinnost bezpečnostních složek více států. Poměr a strukturu nejčastěji zastoupených deliktů přibližuje následující graf.



Obecně vysledovatelným trendem je právě nárůst podvodných aktivit v prostoru informačních technologií, mezi které patří např. prodej neexistujícího zboží, krádeže virtuální identity (mj. tzv. phishing), krádeže údajů z platebních karet či neoprávněné přístupy k cizím účtům. Ve srovnání s rokem 2011 narostl počet podvodů prováděných přes počítač téměř o polovinu (ze 720 na 1039).

Nutno říci, že o velkém množství tohoto typu podvodné činnosti se policie vůbec nedozví, neboť oběť podvodu mnohdy celou událost nenahlásí. Podobná situace přitom platí i v případě závadového obsahu internetu, neboť Policie ČR v současné době nemá personální kapacity k provádění aktivního monitoringu celé veřejné sítě. V tomto směru bylo velkým posunem zahájení provozu on-line formuláře na internetových stránkách policie, který umožňuje jednoduše a rychle nahlásit problematický obsah či aktivity na internetu. Ke spuštění této hot-line k hlášení internetové kriminality došlo 1. srpna 2012.

Následující graf zachycuje celkový meziroční nárůst případů informační kriminality, které zaznamenala Policie České republiky.



Údaje z grafu neznamenají jen setrvalý nárůst samotných případů počítačové kriminality, který logicky roste souběžně s pokračující penetrací informačních technologií do běžného života společnosti. Tato čísla odrážejí také zlepšující se práci policie, která se na tento rostoucí fenomén začíná stále více zaměřovat a postihuje i ty případy, které dříve zůstávaly mimo zorný úhel jakékoliv kontroly. Její možnosti i zkušenosti se navíc s každým rokem zlepšují, což je ovšem vyváženo neustálým pokrokem v této dynamicky se rozvíjející oblasti.

Je to součást celoevropského úsilí začlenit kybernetický prostor, který se dlouho rozvíjel dosti nezávisle a nekontrolovaně, do prostředí práva a odpovědnosti, známého z „reálného“ světa. Tento přístup se stává stále větší nutností ve chvíli, kdy jsou aktivity v kybernetickém prostoru sto ovlivnit onen „reálný“ svět ve stále stoupající míře.

Značný nárůst registruje policie především v případě phishingu. Organizátoři např. zneužití botnetů se sice mnohdy nacházejí v zahraničí, na našem území se ovšem objevují tzv. bílí koně („e-mules“), kteří mají za úkol např. převzít na svůj účet peníze, získané z podvodné činnosti, a dalším kanálem je poslat dál. Stále častější je také zřizování speciálních elektronických obchodů, které jsou vytvářeny primárně za účelem krytí původu financí pocházejících z trestné činnosti (zejména z phishingových útoků či zneužití 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 realizovaných komunikací. Zde je patrná absence pravidel, která jsou již nyní aplikována na služby elektronických komunikací. Obdobným mechanismem jsou pak kryty i iniciace a správy elektronických finančních transakcí.

Jsou detekovány i výskyty krádeží identit, které jsou zneužívány buď ke kompromitaci faktických subjektů, anebo využity jako legendy pro páchání 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.

Aktivity bezpečnostních složek a státní správy

V současné době se na Policejním prezidiu ČR připravuje materiál s názvem „Koncepce rozvoje schopností Policie ČR vyšetřovat informační kriminalitu“, která vzniká jako součást Koncepce boje proti organizovanému zločinu, přičemž tento materiál systémově nastavuje budoucí podmínky pro efektivní odhalování a vyšetřování kybernetických incidentů.

Na poli mezinárodní spolupráce jsou v současné době dokončovány přípravy k ratifikaci Mezinárodní úmluvy o počítačové kriminalitě Českou republikou, důležité je také vytvoření Evropského centra pro kybernetickou kriminalitu, ke kterému dojde v lednu 2013, a které bude zastřešeno centrálou Europolu. Centrum by mělo poskytovat podporu pro vyšetřování i stíhání členským státům, školit národní experty a udržovat online databázi kyberkriminality i kybernetický zločinců.

V oblasti kybernetické bezpečnosti je nutné připomenout přechod gesce nad touto problematikou z Ministerstva vnitra na Národní bezpečnostní úřad, ke kterému došlo na základě Usnesení Vlády ČR č. 781 ze dne 19. října 2011. Na základě tohoto Usnesení vznikla Rada pro kybernetickou bezpečnost, která se naposledy sešla dne 28. listopadu 2012. NBÚ také vypracoval novou Strategii pro oblast kybernetické bezpečnosti České republiky a Akční plán opatření k této Strategii, v tomto případě pro léta 2011-2015. V obou těchto dokumentech se objevuje řada podstatných úkolů, které stanovují směřování České republiky při zajišťování kybernetické bezpečnosti v příštích letech.

Usnesením č. 382 z 30. května 2012 vláda schválila věcný záměr Zákona o kybernetické bezpečnosti a uložila řediteli Národního bezpečnostního úřadu předložit vládě text návrhu zákona v paragrafovém znění do konce července 2013. Tento zákon je v mnoha směrech průlomový, neboť specificky upravuje důležitou, dosud v českém právním řádu poměrně opomíjenou oblast kybernetické bezpečnosti. V současné době se schází mezirezortní pracovní skupina, která připravuje návrh paragrafovaného znění zmíněného zákona.

Převzetím gesce nad problematikou kybernetické bezpečnosti se NBÚ rovněž zavázal zajistit vznik Národního centra pro kybernetickou bezpečnost (NCKB), které bude mít své sídlo v Brně. NCKB zahájilo 1. září 2012 vykonávání základních činností Vládního CERTu, tj. dohled nad sítěmi veřejné správy a samosprávy. Pracoviště provozuje webové stránky govcert.cz, zpracovalo již několik zahraničních požadavků na spolupráci při řešení kybernetických bezpečnostních incidentů a bylo zapojeno do cvičení Severoatlantické aliance Cyber Coalition 2012.

Kromě výše zmíněných aktivit veřejné správy existuje rovněž řada programů, zaměřujících se na osvětovou činnost a pomoc uživatelům internetu při bezpečném pohybu na síti. Z těchto iniciativ je možné zmínit zejména stránky bezpecnyinternet.cz a saferinternet.cz, které poskytují především mladistvým a dětským uživatelům internetu (a jejich rodičům) cenné rady a poukazují na rizika spojená s používáním internetu (např. pohybem na sociálních sítích). Zároveň je na stránkách horka-linka.cz provozováno kontaktní centrum, které přijímá hlášení týkající se nezákonného obsahu na internetu (zejména zneužívání dětí), zatímco na portálu pomoconline.cz lze nalézt krizové centrum, pomáhající dětským obětem internetové kriminality.

Očekávané bezpečnostní hrozby a trendy pro rok 2013

Uplynulý rok 2012 jen potvrdil nárůst počtu incidentů souvisejících s kybernetickou bezpečností, ke kterému dochází již mnoho let v řadě. Jen pro srovnání, zatímco v roce 2000 kolovalo po světě odhadem asi 11 tisíc škodlivých počítačových kódů, již v roce 2008 překročil počet druhů malwaru celosvětově 1,2 milionu. Neroste ovšem jen počet (exponenciální nárůst z počátku nového tisíciletí se ve skutečnosti zbrzďuje), ale především nebezpečnost a sofistikovanost kybernetických útoků. Také škody narůstají rovnoměrně s tím, jak jsme čím dál větší množství služeb a úkonů přesouvá do virtuálního světa (např. mobilní internetové platby, datové schránky atd.).

Existují příklady mimořádně sofistikovaných virů jako je Flame nebo Stuxnet, na jejichž vývoj muselo být vynaloženo velké množství prostředků, kybernetickému světu nicméně stále dominují programy jednodušší, které mnohdy s velmi malými náklady dosahují poměrně velkého efektu. Způsoby útoků se sice většinou opakují, na následujících řádcích se nicméně zaměříme na hrozby, které se objevily nově, případně se jejich příchod očekává v nejbližší budoucnosti.

Nové hrozby

Zajímavým vodítkem mohou být například **konference Defcon a Black Hat**, které se v právě uplynulém roce konaly v Las Vegas. Počítačoví experti na nich představili mnoho nových či vznikajících ohrožení s potenciálně velmi nepříjemnými dopady. Za jednu z nejproblematičtějších oblastí moderního hackingu byla označena **pokročilá technika obcházení počítačového zabezpečení (tzv. AET)**, která dokáže přelstít i moderní firewally. Ty dokáží poměrně spolehlivě odhalit škodlivý kód, který se pokouší vniknout do počítače. Současní hackeři jsou nicméně schopní tento kód rozdělit na řadu menších sekvencí, které mohou projít zabezpečením nepovšimnuté a poté se opět složit a aktivovat. Dílčí části malwaru totiž firewally zatím odhalit nedokáží. Útoky tohoto typu jsou prozatím poměrně málo časté, protože vývoj těchto sofistikovaných typů kódů je náročný. S rozvojem technologií se ale usnadňuje a zlevňuje a riziko spojené s tímto typem útoků tak bude podle všeho v budoucnosti narůstat.

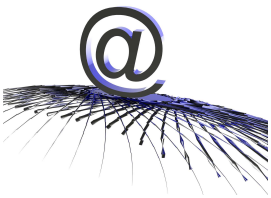
Konference také upozornila na **značné riziko zavirovaných hardwarových produktů**, které se v poslední době velmi rychle šíří. Do některých částí hardwaru (např. do síťových karet) může být již předem naprogramován jakýsi tajný vchod, který po instalaci tohoto zařízení zpřístupní váš počítač hackerům. Jelikož je tento škodlivý přístup přímo fyzickou součástí počítače, snadno se dostane přes jakákoliv softwarová zabezpečení a firewally, jelikož přes ně vůbec neprochází. Jediným řešením je nákup všech součástí počítače pouze od ověřeného a licencovaného výrobce, který nejlépe provádí pravidelné bezpečnostní audity. To může být řešením pro velké firmy ale běžný zákazník se jen velmi těžko dozví, odkud jeho hardware skutečně pochází, protože tyto problematické padělky se mnohdy dostávají různými cestičkami do běžné distribuce a kamenných obchodů. I originální hardware může být kdekoliv během své cesty od výrobce k zákazníkovi upraven tak, aby sloužil nelegálním účelům.

Konference upozornila také na další nové, poměrně pozoruhodné riziko, které by mohlo znamenat návrat ke prastarým technologiím zámku a klíče v cestovním průmyslu. Řada hotelů po celém světě totiž používá u vchodů do pokojů zámky elektronické, které se otevírají s pomocí plastové kartičky. Nejméně jeden výrobce ale má ve svém typu zámků zranitelnost, která umožňuje otevřít dveře s pomocí notebooku, a to doslova během několika vteřin. **Hacker dokáže s pomocí jednoduchého zařízení, které se dá sestavit z běžně dostupných dílů, přečíst bezpečnostní kód zámku a zadat příkaz k otevření**. Odhadem tak po světě existuje pro takového člověka velmi snadný přístup do asi 4 milionů zámků. Pozoruhodné na celém případu je fakt, že výrobce zámků požaduje po odhalení problému po hotelech a dalších svých zákaznících peníze na vydání bezpečnostní záplaty.

Na konferenci byly diskutovány i další velmi rozšířené zranitelnosti jako je zneužití Javy nebo zastaralého, ale stále hojně používaného VPN softwaru. Objevily se také úvahy o možnosti napadení systému řízení letového provozu či bezpečnostních kamer, ty lze ale prozatím odkázat do roviny spekulací, neboť takové útoky dosud nikdo nebyl schopen úspěšně demonstrovat.

Rizika spojená s mobilními zařízeními

Jaké budou tedy hlavní trendy bezpečnostních hrozeb v nadcházejícím roce 2013? Tím nejočekávanějším z nich, který má také největší potenciál rozvoje ve střednědobém horizontu, je **pokračující přesun pozornosti od klasických počítačů k mobilním zařízením. Dosud hackeři soustřeďovali ve svých aktivitách především na běžná PC, nástup a masové rozšíření tzv. „chytrých" telefonů a tabletů jim ale otevřel zcela nové pole působnosti.** V průběhu roku 2012 to velmi dobře ukázal například úspěch viru Eurograbber, kterému se podařilo z účtů klientů různých bank po celé Evropě převést téměř miliardu korun. Tento virus totiž napadá zároveň klientův počítač i mobil, čímž se mu daří obcházet autorizaci on-line platby pomocí SMS. Něco takového by nebylo u starého telefonu bez přístupu na internet možné, a autorizační kód zaslaný na mobil tak platil za poměrně spolehlivý bezpečnostní prvek. Tomuto případu se podrobněji věnuje předchozí kapitola o bankovnictví a finanční bezpečnosti.



V současnosti existuje podle odhadů společnosti FortiGuard Labs zhruba 50 tisíc škodlivých kódů cílících na mobilní zařízení. V příštím roce se očekává jejich exponenciální nárůst, takže mobily postupně v hackerském zájmu vyrovnají či předčí klasické počítače, kde je „trh s malwarem" daleko více nasycen, takže již neroste tak dramaticky jako v průběhu uplynulé dekády.

Jedním z hlavních způsobů, jakým se bude škodlivý software do mobilů dostávat, budou infikované aplikace. V této oblasti se očekává dramatický nárůst hackerské aktivity. **Objeví se nejen další fiktivní app story, ale nakažené programy se ve větší míře dostanou i do oficiální on-line distribuce**. Uživatel by si měl začít dávat větší pozor, zda aplikaci skutečně nakupuje v oficiálním obchodě, nebo se stal obětí phishingu. Může se například snadno stát, že se splete při zadávání adresy internetového obchodu (např. místo Google Play zadá Google Plays) a tím se ocitne na zcela identických stránkách plných škodlivého softwaru. Stránek imitujících velké obchody jako je právě Google Play či Apple App Store pravděpodobně přibude, je ovšem pravděpodobné, že infikované aplikace proniknout i na tyto oficiální stránky. Při množství nově nabízených aplikací totiž nebude pro velké obchody možné uhlídat, zda žádná z nich neobsahuje části se škodlivým kódem.

Nebezpečný software se do vašeho telefonu může dostat nejen přes aplikace, ale využitelná je v podstatě celá škála triků známých z klasických osobních počítačů. Časté je a bude šíření malwaru pomocí infikovaných webových stránek, hackerům se podařilo ovládnout i celé servery, které pak rozesílají výzvy ke stažení škodlivého kódu a navíc shromažďují ukradená data. Značný nárůst v minulém roce zaznamenal počet automatizovaných botnetů. **Velkým trendem roku 2012, a také nemalým rizikem, je skladování dat v cloudu**. Právě u mobilů, jejichž hardwarová paměťová kapacita bývá omezená, je tento typ archivace dat velmi oblíbený. Různé incidenty postihly v minulém roce snad všechny velké firmy poskytující cloudové služby – Dropbox, Linkedln, Yahoo!, Formsprings. Mnohdy sice nestálo za únikem dat jejich zavinění (data unikla od třetích osob), ale tyto incidenty upozorňují na rizikovost nových technologií a nutnosti je využívat s přiměřenou dávkou opatrnosti. Únik informací postihl loni také velké společnosti vydávající kreditní karty – Visa a MasterCard. Zmiňovaný incident ovlivnil celkem více než 50 tisíc účtů, přičemž u 876 z nich skutečně došlo k pokusu o podvod.

Tímto (a nejen tímto) způsobem se může do telefonu dostat hned několik typů malwaru. **V roce 2012 byl vůbec nejčastějším typem ten, který pobyt v mobilu využíval k distribuci SMS zpráv na prémiová čísla.** O takové aktivitě se přitom uživatel dozvěděl až společně

s astronomickým účtem od svého operátora. **Tento typ malwaru tvořil asi 40% z celkového počtu škodlivých mobilních programů.** Mezi další nejčastější typy patří tzv. spyware, který krade a odesílá data (využitelná jak pro krádež vašich peněž, tak např. v průmyslové špionáži), případně malware, který vaše zařízení přemění v tzv. zombie. Takový telefon pak může pachatel na dálku ovládat. Může do něj instalovat další škodlivé kódy a z vaší IP adresy je rozesílat (zajímavým příkladem může být zatčení tří Japonců z tohoto roku, z jejichž infikovaných počítačů neznámý pachatel rozesílal teroristické výhružky – viz přehled událostí na začátku této kapitoly). Má také možnost z něj krást data, měnit jeho konfigurační parametry atd.

Další možné hrozby v příštím roce

Mobily budou pro kybernetické zločince skutečně velmi lákavým cílem. Důvod je zřejmý – slibují vidinu obrovských zisků s poměrně malým rizikem odhalení a usvědčení. V roce 2011 používalo mobilní verzi internetového bankovnictví asi 300 milionů uživatelů, podle odhadů překročí jejich počet v roce 2013 hranici půl miliardy. Stále rozšířenější jsou také mobilní peněženky. Například společnost Starbucks spustila svou aplikaci na platbu za kávu v roce 2011 a během pouhých 11 měsíců zaznamenala 42 milionů mobilních nákupů. Pro mnoho lidí představuje tento způsob platby vítané zjednodušení, pro hackery ale také velkou příležitost, zvláště v době, kdy je tato technologie ještě v plenkách a nebyly odhaleny všechny její zranitelnosti.

Pozor na tablety

Mezi ohrožená mobilní zařízení nicméně nepatří jen „chytré“ telefony, ale také tablety. Jejich obliba velmi rychle roste (v roce 2012 se jich na celém světě prodalo zhruba 120 milionů), míra jejich zabezpečení přitom pokulhává ještě více, než v případě mobilů. Při konferencích tablety často nahrazují notebooky, díky svým multimediálním schopnostem, rozměrům i delší výdrži baterie. Obsahují tak mnohdy citlivá firemní či soukromá data. Je proto důležité si uvědomit, že tablety je proti zneužití nutné chránit podobným způsobem, jaký se pro ochranu používá u stolních počítačů či mobilních telefonů (tj. vybavit je antivirovými programy a dalším bezpečnostním softwarem a počínat si s patřičnou opatrností). Pro statistiky týkající se mobilního malwaru doporučujeme čtvrtletní zprávy společnosti McAfee na stránkách www.mcafee.com.

Dalším možností, jak zneužít cizí mobilní telefon k nekalým účelům, jsou falešné bezdrátové sítě. Ty se již během roku 2012 na mnoha místech začaly objevovat a lze očekávat, že v příštím roce bude tento fenomén dále růst. Je velmi snadné vytvořit veřejně přístupnou Wi-Fi síť, která bude vypadat podobně jako například veřejně přístupné sítě, jaké známe z letišť, restaurací či kaváren. Hacker tak získá přístup k veškerým datům, která přes tuto síť odešlete, včetně mailů, ale také například přístupu k internetovému bankovnictví. Bezpečnostní doporučení je jednoduché – připojujte jen k těm Wi-Fi sítím, jejichž původ dobře znáte (i ta ovšem může být zneužita, pokud nemá dostatečné zabezpečení), případně raději nikdy neposílejte citlivá či zneužitelná data přes veřejnou síť. Rozšíří se také počet falešných aktualizací, skrze které se opět může váš mobilní telefon infikovat malwarem.

Jedním z poměrně nových fenoménů ve světě hackingu je také snaha o manipulaci internetových vyhledávačů. Hacker pak může ovlivnit výsledky vyhledávání a podat uživateli přednostně ty odkazy, které uzná za vhodné (například ty, obsahující malware). Jen málokdo totiž po zadání klíčových slov do vyhledávače prohlíží výsledky i z jiné, než první či druhé nalezené stránky.

V příštím roce se očekává prudký nárůst počtu infikovaných zařízení tzv. ransomware, který nejprve zašifruje některé soubory na disku uživatele a následně za klíč k nim vyžaduje vysoké "výkupné". Vyskytly se i případy, kdy za klíč bylo požadováno 3 tisíce dolarů s výhružkou, že v případě nezaplacení budou data zaslána policii. Pro uživatele je tento typ malwaru jen těžko odhalitelný a současné statistiky předpovídají alarmující nárůst tohoto trendu v oblasti kyber kriminality.

Fenomén BYOD

Další hrozby pro rok 2013 lze očekávat v souvislosti s rozšiřujícím se fenoménem BYOD (zkratka *Bring Your Own Device*). V jeho rámci firmy podporují své zaměstnance, aby si do práce nosili svá vlastní elektronická zařízení (notebooky, tablety), případně na nich vykonávali práci z domova. I v České republice jde o populární novinku, která má řadu výhod – mezi největší z nich patří snižování nákladů pro firmy a pro zaměstnance zase možnost nebýt při práci tak přísně vázán na vlastní kancelář a možnost práce na vlastním, důvěrně známém zařízení. Jako obvykle má ale i tento přístup nemalá bezpečnostní rizika. **Podle údajů americké společnosti Webroot se více než dvě třetiny (67%) firem používajících systém BYOD potýkalo s problémem ztráty či krádeže mobilního zařízení (a s tím související možností zneužití dat), 32% zase zaznamenalo nákazu malwarem**.

Při použití BYOD jsou paradoxně velké firmy ohroženy stejně, jako ty menší. Malé společnosti si nemohou dovolit tak velké investice do bezpečnostního softwaru, šifrování, dvoufaktorové autorizace atd. a stávají se tak snazším terčem pro hackery. Podle Webroot se dokonce jen asi 40% firem s méně než 100 zaměstnanci nějakým způsobem stará o bezpečnost mobilních zařízení. **Velké společnosti jsou sice obecně zabezpečeny lépe, nicméně při velkém počtu pracovníků je při využití BYOD prakticky nemožné uhlídat, zda všichni zaměstnanci veškerá bezpečnostní opatření skutečně dodržují, zvlášť když svá zařízení používají i k soukromým účelům**. Navíc se při vyšším množství zaměstnanců zvyšuje i pravděpodobnost, že některý z nich svůj mobil či notebook ztratí, nebo mu bude ukraden. Velké firmy jsou navíc mnohem lákavějším cílem, protože jejich data jsou obvykle cennější. Ne všechny firmy přitom pro ochranu svých dat používají dostatečně pokročilé způsoby šifrování (pokud vůbec nějaké používají). Například u finančních či bezpečnostních institucí může takové ztracené či odcizené zařízení představovat velmi vážný problém.

Z tohoto důvodu přistoupila řada firem, které začaly BYOD využívat, k postupnému omezování přístupu k citlivým firemním aplikacím z těchto soukromých zařízení. Podle Ping Identity například finanční instituce zpřístupňují v rámci systému BYOD asi jen polovinu aplikací, které zaměstnanci při své práci využívají, což výhody celého principu poněkud omezuje. Velké firmy navíc začínají ve stále větší míře využívat šifrování (které po odcizení zařízení znemožní zneužití dat) a dvoufaktorovou autorizaci (kdy je pro přístup do citlivé aplikace vyžadováno nejen klasické heslo, ale i další autorizační kód generovaný jiným zařízením).

Sociální inženýrství

Jednou z nejjednodušších metod jak získat přístup k citlivým datům je přitom využití tzv. sociálního inženýrství. Pro získání citlivých dat není nezbytně nutné překonávat složitá bezpečnostní opatření, někdy stačí se zaměstnance prostě zeptat. Na konferenci Defcon byla prezentována demonstrace telefonátu do jedné velké firmy, kdy se volající „hacker“ vydával za jednoho ze zaměstnanců, který si potřebuje přes víkend dodělat nějakou práci, ale zapomněl některé důležité informace pro vzdálený přístup. Jeho nic netušící „kolega“ mu během deseti minut prozradil množství citlivých informací, včetně přístupového hesla. Na důvěřivosti a neopatrnosti některých pracovníků tak mohou ztroskotat i ta nejsofistikovanější softwarová bezpečnostní opatření. Ostatně celý obrovský fenomén phishingu je založen na stejném principu – **výrazně snazší, než pokoušet se vypáčit kvalitní zámek na pancéřových dveřích, je přesvědčit někoho uvnitř, aby vám otevřel**.

Firmy i instituce měli mít na paměti, že ani perfektní technické zabezpečení nemusí být k ničemu, pokud jejich vlastní zaměstnanci nemají povědomí o bezpečném pohybu v kyberprostoru.

Pracovníci by tak měli být pravidelně školeni a informováni o nových bezpečnostních hrozbách. Velké množství malwaru se do sítí soukromých společností dostává tak, že jejich zaměstnanci otevřou infikovaný soubor, který jim přijde mailem, případně kliknou na podezřelý odkaz.

Výrazně rostoucím fenoménem je v tomto směru tzv. **spear phishing**, kdy je podvodná zpráva **přizpůsobena na míru danému uživateli**, který tak jen velmi těžko zjistí, že jde o podvod. Jinými slovy se jedná o personifikovaný útok, kdy útočník oslovuje adresáta jménem, uvádí jeho skutečnou pozici ve firmě, případně využívá další informace, které získal např. na firemních stránkách či sociálních sítích. Většinou se jedná o emaily s infikovanou přílohou či odkazem na nebezpečné stránky. Antivirové a antispamové programy přitom tento typ útoků většinou neumí odhalit, a proto skutečně záleží především na internetové gramotnosti koncového uživatele, zda útoku podlehne, či nikoliv.

Exkurz: Rudý říjen

Firmě Kaspersky Labs se nedávno podařilo objevit nový špionážní malware, který je svou sofistikovaností přirovnáván ke slavnému viru Flame. O vyspělosti nové kampaně, která dostala název Rudý říjen (zkráceně Rocra), svědčí i fakt, že byla odhalena až nyní, přestože trvá již nejméně pět let (od roku 2007) a dosud se ji nepodařilo zcela zastavit.

Cloudové útoky
nová šance pro hackery

Nedávný útok na stránky amerických bank (o kterém se zmiňujeme v monitoringu vybraných událostí), dokázali íránští hackeři úspěšně provést i přesto, že o něm předem informovali a napadené instituce tak měly trochu času se na jejich akci připravit. Jedním z důvodů, proč se jim to podařilo byl fakt, že útok typu DDoS (Distributed Denial of Service), jejichž principem je přetížení a následný kolaps napadených stránek, neprováděli z běžných počítačů, ale daleko účinnější metodou ovládnutí celých datacenter (cloudy), které přeměnily ve vysokokapacitní útočící počítače. Intenzita takového útoku pak řádově převyšuje klasické akce prováděné z běžných počítačů, jaké provádějí např. jejich kolegové z Anonymous. Proti tomuto typu útoků dosud neexistuje účinná obrana, a tak se dá očekávat, že bude cloudových ataků přibývat.

Rudý říjen funguje jako velmi pokročilý spyware – umožňuje sbírat data z pevných i externích disků, mobilních zařízení, ale také emaily a přístupové údaje do utajených počítačových systémů. Velmi pozoruhodný je fakt, že se soustředila také na zašifrované soubory, především ty vytvořené kryptografickým systémem Acid Cryptofiller, používaný NATO a od léta 2011 i většinou orgánů EU. Virus navíc dokázal využít ukradená data z infikovaných sítí k napadení dalších, které s nimi byly ve spojení.

Celkově byly podle Kaspersky Labs infikovány stovky počítačů, nejčastěji v Rusku a ve východní Evropě, řada obětí se ale nachází i v Německu, USA a podle všeho se virus vyskytl i v České republice. Některé indicie naznačují, že Rocra byla naprogramována rusky hovořícími osobami (např. změna základního kódování stránky v nosiči trojského koně, které se obvykle používá pro zobrazení azbuky). Rocra se zpočátku šířil hlavně přes email prostřednictvím spear phishingu, někdy využíval i bezpečnostní trhliny a ukradená hesla. Infikované počítače odesílaly svá citlivá data přes C&C servery, konečného adresáta se ale stále nepodařilo vystopovat.

Hlavním záměrem byl zřejmě sběr tajných informací, zejména v energetických a jaderných institucích a dále v obchodních a leteckých společnostech. Infekce napadla i řadu vládních sítí a organizací a rovněž vědecké instituce. Drtivá většina takto napadených počítačů se nacházela v zemích bývalého SSSR. Kaspersky Labs ve spolupráci s některými národními CERT týmy pokračuje ve vyšetřování Rocra a vydal také blokační záplatu s názvem Backdoor.Win32.Sputnik.

Zdroje: eset.cz, govcert.cz, businessworld.cz, itbiz.cz, infoworld.com, europa.eu computerworld.cz, net-security.org, novinky.cz, mcafee.com, itnewsafrica.com, scmagazine.com.au, businessinsider.com

Vybrané události ve sledovaném období

Září

Zřízen evropský tým CERT

V rámci zintenzívnění boje proti počítačové kriminalitě zřídily instituce EU stálý tým pro reakci EU na nouzové počítačové situace (Computer Emergency Response Team čili CERT-EU). K tomuto rozhodnutí došlo po úspěšné jednoroční pilotní fázi týmu. CERT má chránit před kybernetickými útoky zejména instituce a orgány Evropské unie.

V rámci Digitální agendy pro Evropu přijaté v květnu 2010 se Komise zavázala zřídit CERT pro instituce EU jako součást celkového závazku na posílení a zvýšení úrovně politiky EU v oblasti bezpečnosti sítí a informací v Evropě. Digitální agenda také vyzývá všechny členské státy ke zřízení sítě národních a vládních týmů CERT po celé EU do roku 2012.

Národní centrum kybernetické bezpečnosti zahájilo činnost vládního CERTu

Nové Národní centrum kybernetické bezpečnosti (NKCB), vybudované v Brně, začalo od 1. září 2012 pracovat jako tzv. vládní CERT. Toto pracoviště bude tudíž zodpovědné za ochranu a bezpečnostní podporu datových sítí provozovaných státní a veřejnou správou. Zároveň by se mělo podílet i na zvyšování vzdělanosti v oblasti bezpečnosti na internetu. Vybudování tohoto centra bylo uloženo Národnímu bezpečnostnímu úřadu, na základě vládního usnesení z roku 2011. Pracoviště provozuje webové stránky www.govcert.cz. Od svého vzniku přijalo již několik zahraničních požadavků na spolupráci při řešení kybernetických bezpečnostních incidentů a bylo zapojeno do cvičení Severoatlantické aliance Cyber Coalition 2012.

Nová evropská strategie na podporu cloud computingu

Nová strategie Evropské komise pro „uvolnění potenciálu cloud computingu v Evropě“ uvádí opatření, která mají do roku 2020 zaručit čistý přírůstek 2,5 milionu nových evropských pracovních míst a roční nárůst HDP v EU ve výši 160 miliard EUR (přibližně 1 %).

Cílem této strategie je urychlit a posílit využívání cloud computingu ve všech odvětvích hospodářství.

Cloud computingem se rozumí ukládání údajů (např. textových souborů, obrázků nebo videí) a softwaru na vzdálených počítačích, k nimž mají uživatelé přístup prostřednictvím internetu ze zařízení, které si sami zvolí. Dnes zveřejněná strategie navazuje na návrh aktualizace pravidel pro ochranu údajů, který Komise předložila v roce 2012, a předchází evropské strategii pro kybernetickou bezpečnost, jejíž návrh má být předložen v nadcházejících měsících. Výhody cloud computingu jsou dány jeho úsporami z rozsahu. 80 % organizací, které zavedly cloud computing, dosahuje nejméně 10–20% úspor nákladů. Bude-li cloud computing přijat ve všech odvětvích ekonomiky, lze rovněž očekávat významné zvýšení produktivity.

V současné době odrazuje mnoho potenciálních uživatelů od přijetí cloud computingu neexistence společných norem a jasných smluv. Poskytovatelé a uživatelé cloud computingu rovněž požadují jasnější pravidla, pokud jde o poskytování služeb cloud computingu, například v otázce soudní příslušnosti v případě právních sporů nebo záruk umožňujících snadné předávání údajů a softwaru mezi různými poskytovateli cloud computingu. Tento způsob ukládání informací je nicméně často zmiňován také v souvislosti s možnými bezpečnostními riziky.

Kvůli špatně zabezpečenému systému unikla data společnosti ČEZ

Za předčasným únikem části hospodářských výsledků energetické skupiny ČEZ stojí nedostatečné zabezpečení části vnitřního internetového systému firmy. Výsledky včera předběžně zveřejnila agentura Reuters. "Došlo k prolomení systému a stažení části informací z naší jedné IP adresy," vysvětluje incident finanční ředitel skupiny ČEZ Martin Novák. Šlo tedy o útok na publikační část serverů ČEZu, a to z jediné IP adresy, která je registrovaná na Reuters.

Podobný systém jako ČEZ přitom používá většina firem, záležitost pro ně může být poučením do budoucna. Podle mluvčího společnosti ČEZ Ladislava Kříže je firma vystavena během půl roku přibližně deseti hackerským útokům. "Žádný hacker se ještě nikdy nedostal do vnitřních systémů firmy, jako je obchodní nebo provozní," poznamenal však Kříž. "Kolegům z Reuters se podařilo dostat na neveřejné stránky, které jsou naplněny informacemi veřejnými, ale teprve připravenými k publikování," dodal Kříž.

Říjen

Proběhlo cvičení Cyber Europe 2012

Stovky odborníků na kybernetickou bezpečnost z celé EU si vyzkoušeli svou připravenost čelit kybernetickým útokům v celodenní simulaci celoevropského rozsahu. V rámci akce Cyber Europe 2012 celkem 400 expertů z předních finančních institucí, telekomunikačních společností, poskytovatelů internetových služeb a místních a centrálních vlád z celé Evropy bojovalo s více než 1 200 na sobě nezávislých kybernetických incidentů (včetně více než 30 000 e-mailů). Během simulovaného útoku spočívajícího v tzv. distribuovaném odepření služby (*distributed denial of service*) se testovalo, jak by reagovali a spolupracovali v případě trvajícího koordinovaného útoku na veřejné webové stránky a počítačové systémy předních bank. Podobný útok, kdyby k němu skutečně došlo, by vedl k masovému narušení systémů, které by poškodilo miliony občanů a podniků po celé Evropě, a způsobil by milionové ztráty evropské ekonomice.

Kybernetické incidenty jsou čím dál častější. V roce 2011 vzrostl počet útoků na webové stránky o 36 % a počet společností, které mezi roky 2007 a 2010 nahlásily bezpečnostní incidenty spojené s finančními ztrátami, vzrostl čtyřikrát (z 5 % v roce 2007 na 20 % v roce 2010). Podle odhadů expertů Světového ekonomického fóra existuje 10% riziko, že v příští dekádě dojde k zásadnímu incidentu s dopadem na klíčovou informační infrastrukturu, který způsobí hospodářské škody v hodnotě více než 200 miliard eur. Simulační cvičení se odehrálo v uzavřeném systému, který simuloval vlastnosti a provoz reálných klíčových informačních infrastruktur. Nedotklo se žádné skutečné infrastruktury. Výsledky cvičení je možné nalézt na stránkách Evropské agentury pro bezpečnost sítí a informací ENISA.

Hackeři z Anonymous napadli weby švédských státních institucí

Hackeři dnes vyřadili z provozu několik webů švédských státních institucí. V prohlášení podle zpravodajského serveru The Local uvedli, že jde o odplatu za razii u poskytovatele internetových služeb PRQ, který dříve hostil The Pirate Bay, portál odkazující na nelegální hudbu a filmy, a WikiLeaks. Po odpoledním útoku pirátů nefungovaly kromě několika stránek úřadů také portály centrální banky, parlamentu, tajné služby Säpo nebo prokuratury. Hackeři podle všeho použili takzvanou DDoS metodu, při které záplavou požadavků zahltí cílové servery, které se pak pod náporem zhroutí.

Hackerská skupina Anonymous opakovaně varovala, že chystá odvetu za policejní zásah v PRQ. Policie při něm zabavila tři servery, z nichž jeden obsluhoval stránku Tankafetest.se, která umožňovala sdílení souborů, především filmů, hudby a softwaru. Mezinárodní volné sdružení hackerů Anonymous napadá počítače vlád a dalších institucí po celém světě. Bojuje mimo jiné proti dohledu úřadů a států nad internetem.

Rusko posiluje cenzuru internetu a zřizuje seznam zakázaných webů

Premiér Dmitrij Medveděv podepsal na konci října vládní výnos o zřízení evidence internetových stránek se škodlivým obsahem. Tyto stránky budou muset ruské úřady povinně blokovat. Oficiálním důvodem je ochrana dětí, nevládní organizace a opozice se ale obávají politického zneužití tohoto nařízení, které začalo platit od 1. listopadu 2012. Odpovědnost za blokování nesou poskytovatelé přístupu do internetové sítě, správcem a garantem seznamu je organizace Roskomnadzor, která v Rusku funguje jako dohlížecí orgán v oblasti telekomunikací a informačních technologií. Za zakázané jsou označovány hlavně informace o výrobě narkotik, návody k sebevraždám či dětské porno.

Íránští hackeři provedli další útoky na americké banky

Íránští hackeři v říjnu opět několikrát zaútočili na webové stránky amerických bank a další útoky prý chystají. Informoval o tom deník The Wall Street Journal (WSJ). Důvodem je podle něj jednak video urážející proroka Mohameda natočené ve Spojených státech, jež pobouřilo muslimy v mnoha zemích, jednak mezinárodní sankce uvalené z popudu Washingtonu na Írán kvůli jeho jadernému programu.
Podle některých expertů je video pouze zástěrkou, ve skutečnosti se prý může jednat o akce sponzorované íránským státem, prováděné jako odveta za kybernetické útoky proti íránským jaderným zařízením (zřejmě ze strany USA a Izraele). Terčem se staly banky Capital One a BB&T. Stránky banky Capital One a BB&T byly kvůli tomu několik hodin mimo provoz. Hackeři se zároveň tento týden vysmáli americkému ministrovi obrany Leonu Panettovi, který uvedl, že Pentagon vyčleňuje na obranu proti kybernetickým útokům tři miliardy dolarů ročně. "Máme pro pana Panettu návrh," uvedla íránská skupina hackerů na internetu. "Místo utrácení několika miliard, které vám nepomůže, raději z YouTube stáhněte video útočící na islám," dodala. Americká armáda kvůli obraně před útoky na vládní počítače a klíčovou civilní infrastrukturu vytvořila "kybernetické velitelství". Panetta tento týden uvedl, že v případě bezprostřední zahraniční hrozby nevylučuje preventivní úder.

Kanada se přidává k USA a kvůli bezpečnosti odmítá čínské technologie

Kanada nejspíše vyloučí čínského výrobce telekomunikační techniky Huawei Technologies z plánované výstavby zabezpečené vládní komunikační sítě. Jako důvod uvedla možná bezpečnostní rizika technologií Huawei, na něž v pondělí spolu s možným vlivem čínského státu poukázala zpráva výboru amerického Kongresu. Kanadská vláda může s pomocí národní bezpečnostní výjimky ve výběru dodavatelů pro své zakázky diskriminovat zahraniční firmy považované za příliš rizikové, aniž tím poruší pravidla mezinárodního obchodu.
Již předtím americký sněmovní výbor doporučil, aby největším čínským telekomunikačním výrobcům Huawei a ZTE byl uzavřen přístup na americký trh vládních zakázek, úřady blokovaly plány těchto firem na expanzi v USA a americké firmy s nimi neobchodovaly. Podle zprávy americké sněmovny je vzhledem k obavám z hackerských útoků z Číny také zapotřebí, aby vládní počítačové systémy neobsahovaly žádné komponenty vyrobené oběma firmami. Zařízení Huawei a ZTE by podle zprávy mohla být využita k monitorování určitého typu komunikací a mohla by ohrožovat klíčové komunikační systémy v zemi.

Listopad

V Japonsku odhalen nový druh malwaru, který rozesílá teroristické výhružky

Tři lidé byli v Japonsku zatčeni poté, co z jejich počítače odešly výhružné emaily. Teprve později se ukázalo, že počítač zatčených byl nakažen malwarem, který umožňoval vzdálený přístup dosud neznámým hackerům. Zadržení byli následně propuštěni, po skutečných pachatelích se pátrá.
Jde o poměrně nový druh malwaru, který z napadeného počítače rozesílá výhružné emaily, včetně hrozby teroristickým útokem. Podle analýzy společnosti Symantec se v těchto mailech objevila například prohlášení o přípravě spáchání masové vraždy, bombových útoků na náboženské objekty, či varování mateřské školce, do které chodí jedno z dětí z královské rodiny. Jiný email byl odeslán letecké společnosti a vyhrožoval umístěním bomby v letadle. Konkrétní indicie naznačují, že malware vznikl přímo v Japonsku, nelze ale vyloučit, že se podobné pokusy rozšíří i do dalších zemí.

Nejrozšířenějším malwarem konce roku 2012 zůstal INF/Autorun

Společnost ESET zveřejnila v listopadu statistiky nejčastějších malwarů. Již šestý měsíc v řadě zůstával nejrozšířenější celosvětovou hrozbou INF/Autorun. Tentokrát dosáhl podílu 5,30 %, v Evropě pak obsadil celkové druhé místo s 3,66 %.

INF/Autorun představuje různé druhy malwaru využívající jako cestu k napadení počítače soubor autorun.inf. Tento soubor obsahuje příkaz k automatickému spuštění aplikace po připojení externího média (nejčastěji USB flash disku) k počítači s operačním systémem Windows. Na území České republiky byla v říjnu ve větší míře zaznamenána i hrozba Win32/Dorkbot, vir šířící se přes komunikační službu Skype.

Rozšířený ransomware se vydával i za Policii České republiky
Řadě majitelů emailových adres přišel v průběhu tohoto roku tzv. ransomware, tedy škodlivý software, který zablokuje počítač a požaduje zaplacení určité finanční částky. Většinou se přitom vydává za nějakou oficiální instituci, např. zpravodajskou službu či policii. Odbor informační kriminality Policejního prezidia evidoval v tomto roce stovky případů takových útoků. Na napadeném počítači se objevila zpráva s logem PČR s výzvou k zaplacení pokuty za stahování nelegálního obsahu chráněného autorskými právy. Stopy původců tohoto malwaru vedou do východní Evropy, v tuto chvíli ale nejsou konkrétní pachatelé známi.
Společnost AVG nicméně ve své čtvrtletní zprávě oznámila, že nejméně jeden v současnosti kolující ransomware byl vyvinut v ČR.

Prosinec

Na konferenci v Dubaji se nepodařilo prosadit přísnější dohled nad internetem
Snaha prosadit celosvětový dohled nad internetem skončila nezdarem. Na konferenci Mezinárodní telekomunikační unie v Dubaji totiž řada západních zemí odmítla přistoupit na kompromisní návrh, který podle nich dává až příliš velké pravomoci OSN a dalším činitelům. Řada zemí, včetně České republiky, tak nepodepsala závěrečný dokument (neučinily tak mj. například i Spojené státy, Kanada či Austrálie). Nejspornějšími body jednání byla hlavně lidská práva a rozpor mezi bezpečností internetu a jeho cenzurou. Státy se neshodly ale i v otázce regulace spamu nebo v tom, jak používání internetu účtovat a platit. A některým zemím se nelíbilo ani zvětšení vlivu OSN v případě, že by kontrolu nad oblastí internetu převzala Mezinárodní telekomunikační unie. Konference pod hlavičkou Mezinárodní telekomunikační unie (ITU) se v Dubaji konala dva týdny. Jejím cílem bylo dohodnout nová pravidla volání do zahraničí a přenosu dat přes internet. Naposledy se podobná konference konala v roce 1988, tedy v době, kdy byl internet teprve v plenkách.
Podle šéfa české delegace je nesouhlas ČR především důsledkem skutečnosti, že skupina arabských a afrických zemí prosadila požadavky na změny částí textu návrhu Telekomunikačního řádu, které považovaly USA i země Evropské unie za zásadní. "V okamžiku, kdy vůbec zavedete internet do takové mezinárodní dohody, může se vám přihodit, že jednou bude po vašem státě jiný stát chtít, abyste sami prováděli cenzuru internetu, aby k nim nepřišel obsah, který považují za nežádoucí. To je samozřejmě v liberalizovaném a pokročilém světě něco naprosto neakceptovatelného," formuluje české výhrady vůči návrhu dohody vyjednavač Zeman. Ačkoliv další země by dnes měly podpis pod smlouvu připojit, odpor tolika velkých zemí prakticky zaručuje, že smlouva o dohledu nad internetem se příliš dodržovat nebude.

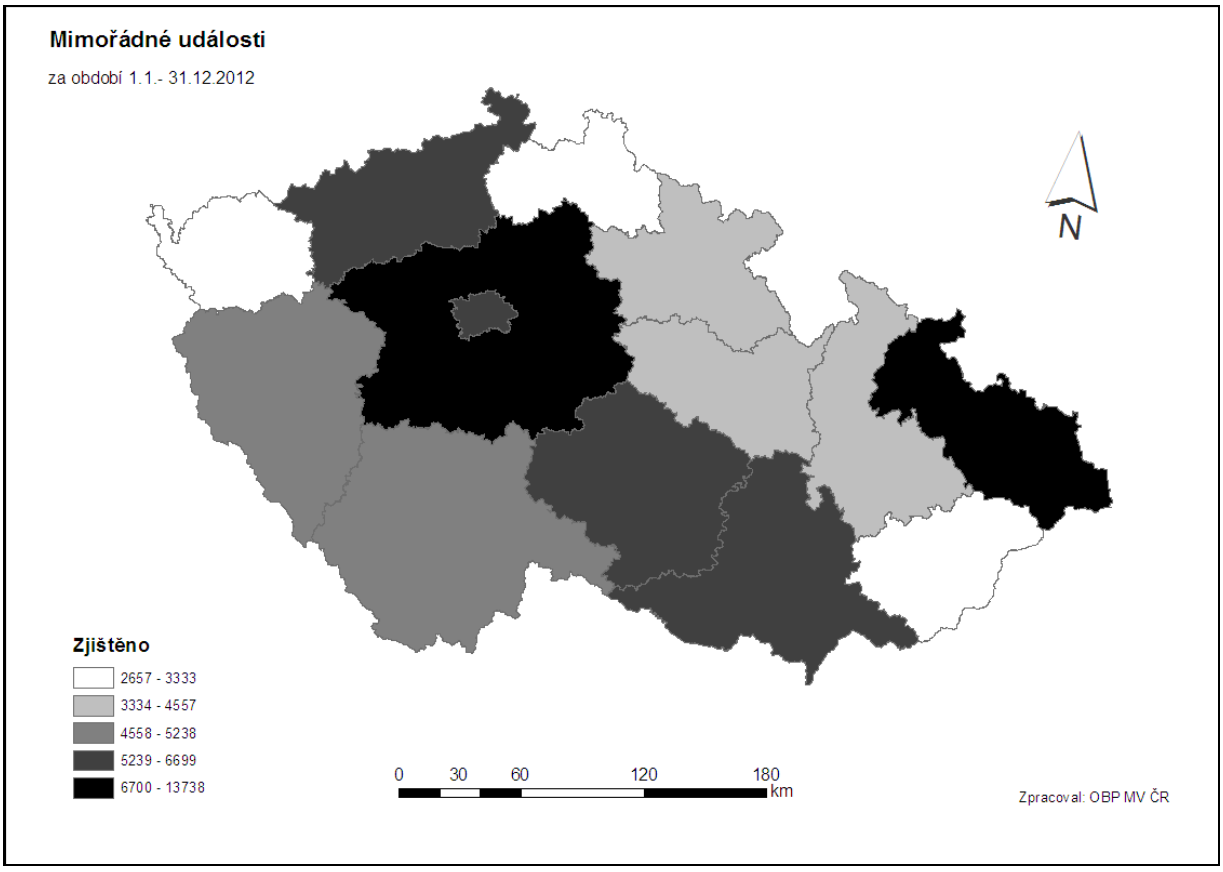
Trojský kůň Boxer se šířil prostřednictvím SMS i v České republice
Trojský kůň SMS Boxer vyvinutý speciálně pro mobilní telefony s operačním systémem Android okrádal obyvatele České republiky a dalších 62 zemí. Potvrdil to nedávný výzkum antivirové společnosti ESET. Mezi nejvíce postižené země patří kromě Česka také Polsko, Německo, Rusko a Francie. "Z Boxera se stal jeden z nejvýznamnějších SMS trojanů loňského roku a je zároveň prvním, který se snaží útočit v tak velkém počtu zemí," říká o hrozbě Petr Šnajdr, bezpečnostní expert společnosti ESET. Analýzu trojského koně zveřejnil ESET nedlouho poté, co SMS zpráva oslavila své 20. výročí. Přesně 3. prosince 1992 byla totiž ve Velké Británii odeslána první textová zpráva ve znění "Veselé Vánoce".
Podstatou tohoto škodlivého kódu je skryté přihlášení mobilního telefonu do zpoplatněných SMS služeb, které provedl infikovaný mobil. Za normálních okolností vidí majitel smartphonu všechny přijaté zprávy, i ty zpoplatněné. V tomto případě však SMS Boxer tyto zprávy zablokoval, uživatel tedy nevěděl, že jeho mobil přijímal zpoplatněné esemesky.

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. – 30.9. 2012 (údaje z posledních třech měsíců roku v tuto chvíli nejsou k dispozici). Tyto statistické výstupy jsou v podrobnější verzi pravidelně aktualizovány rovněž na stránkách www.hzscr.cz.

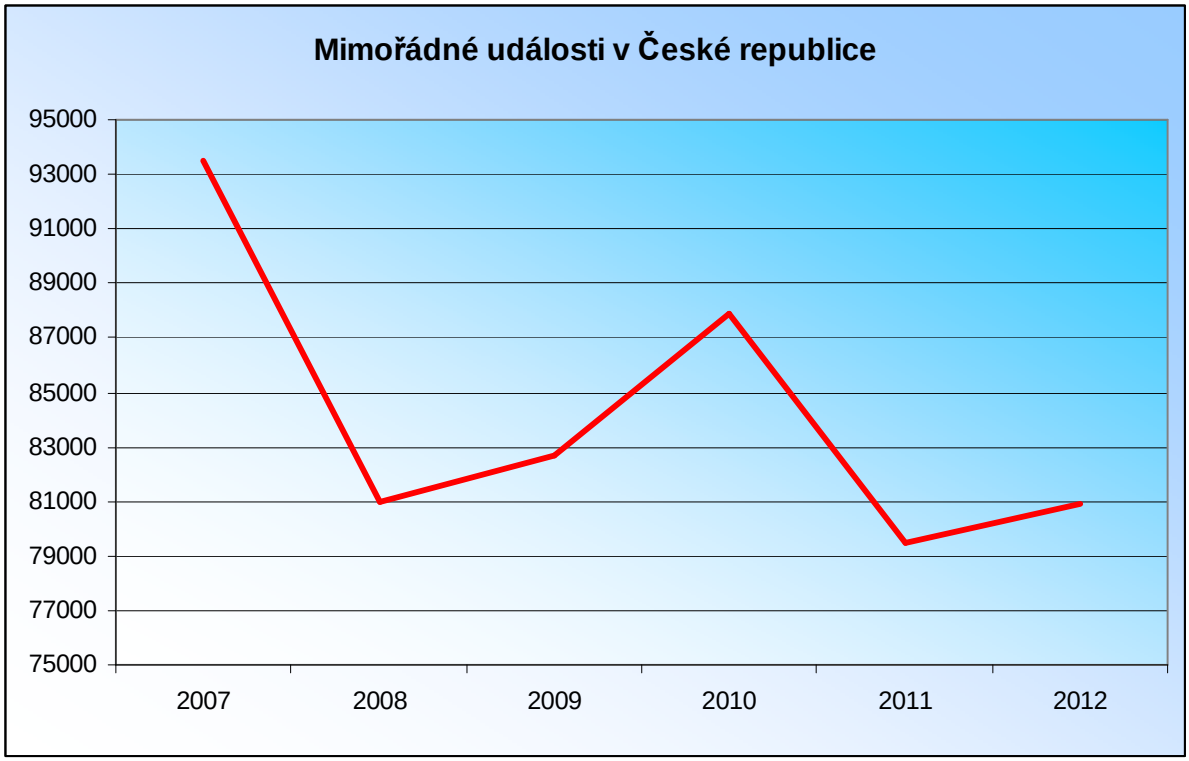
V období od 1. ledna do 30. září 2012 zasahovaly jednotky požární ochrany u 80 894 událostí, což je o 1,8 % více než ve stejném období roku 2011. Nejčetnějšími událostmi byly technické havárie – 50,3 %, následují požáry – 20,2 %, dopravní nehody – 17,0 %, úniky nebezpečných chemických látek – 4,8 %. Rozložení mimořádných událostí podle jednotlivých krajů znázorňuje následující mapa.



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 (např. Ústecký či Olomoucký). Je možné, že se na tom podílejí např. rizikové úseky dálnice D1, nicméně příčiny tohoto stavu by zřejmě vyžadovaly hlubší analýzu.

Nejčastěji museli hasiči zasahovat ve Moravskoslezském a Středočeském kraji, které patří mezi nejlidnatější v zemi. **Moravskoslezský kraj ovšem v tomto ohledu opět vybočuje – došlo zde k celkem 13 738 mimořádným událostem**. Přitom kraj Středočeský, který se umístil v tomto nelichotivém žebříčku na druhém místě, zaznamenal ve zmíněném období „jen“ 9 816 mimořádných událostí, město Praha pak dokonce 6 408. Oproti středním Čechám a Praze (oba tyto kraje jsou přitom lidnatější) si tak Moravskoslezský kraj připsal o téměř 4 tisíce (resp. 7 tisíc) mimořádných událostí více.

Na druhou stranu byl ovšem v Moravskoslezské kraji zaznamenán mírný pokles počtu mimořádných událostí oproti roku 2011, podobně pozitivní trend si připsala i zmiňovaná Vysočina. **Vůbec nejvíc si oproti roku 2011 polepšil kraj Ústecký (-12%), největší, více než čtvrtinový nárůst naopak zaznamenal Liberecký kraj (+26%)**, kde je nicméně celkový počet stále poměrně nízký (3 333). Vývoj počtu mimořádných událostí za poslední roky (za stejné období prvních tří čtvrtin roku) je zobrazen na následujícím grafu.



Z grafu je patrné, že rok 2011 z hlediska nízkého počtu mimořádných událostí jeden z nejúspěšnějších, v roce 2012 se ovšem pozitivní trend poklesu nepodařilo udržet a počty neštěstí začaly opět mírně růst.

Druh události	2010	2011	2012	Index 11/12
Požáry s účastí jednotky PO	13370	16030	16355	102
Dopravní nehody	13277	12214	13757	113
Úniky nebezpečných látek	4288	4142	3890	94
z toho ropných produktů	3605	3313	3046	92
Technické havárie	50783	40771	40666	100
Radiační havárie a nehody	0	1	1	100
Ostatní mimořádné události	5	7	39	557
Plané poplachy	6173	6296	6186	98
UDÁLOSTI CELKEM	**87896**	**79461**	**80894**	**102**

Plané poplachy činí 7,6 % z celkového počtu událostí. Nejvíce událostí bylo v červenci – 15,5 % z celkového počtu, nejméně v lednu – 8,8 %. Podle dnů v týdnu bylo nejvíce událostí ve čtvrtek – 15,0 % a nejméně v neděli – 13,4 %.

Členění zásahů u událostí vyvolaných negativním působením přírodních sil a jevů za období leden – září 2012 je následující:

celkem 7 153 zásahů, z toho:

141 u požárů (způsobených zejména bleskem),

286 u dopravních nehod,

5 při úniku nebezpečné chemické látky,

6 699 u technických havárií,

22 v souvislosti s planým poplachem.

Požáry zaznamenaly oproti stejnému období loňského roku nárůst. Důvodem bylo především jarní období sucha, které se projevilo na počtu požárů volných skládek, odpadů, lesních porostů a požárů v přírodním prostředí vůbec.

Počet dopravních nehod, jejichž následky likvidovaly jednotky PO, loni vzrostl o 13 %. Nejčetnější byly zásahy u dopravních nehod ve Středočeském kraji – 2 227 (+364), minimum bylo v kraji Karlovarském – 387 (+40). Celkově u nehod hasiči bezprostředně zachránili či evakuovali 5 899 osob (+2 770), při zásazích se vyskytlo také 487 usmrcených osob (-7) a 9 794 zraněných osob (+674), jimž v mnoha případech poskytli předlékařskou pomoc.

Z úniků nebezpečných chemických látek byly nejčetnější úniky ropných látek – 3 046 (-267), úniky plynů a aerosolů – 508 (+55), kapalin mimo ropných produktů – 268 (+17), dále pevných látek – 11 (+2) a ostatních včetně potravinářských produktů – 57 (-59). Nejvyšší počet těchto případů byl v hlavním městě Praze – 612 (-2), nejnižší v kraji Pardubickém – 31 (-25).

Kategorie technické havárie zahrnuje technické havárie – 11 (-11), technické pomoci – 36 815 (-692), technologické pomoci – 513 (+1) a ostatní pomoci – 3 326 (+596). Jsou doménou jednotek Hasičského záchranného sboru ČR jako pomoc v nouzi při otvírání uzavřených prostorů, odstraňování překážek na komunikacích, odchytu a likvidaci obtížného hmyzu apod. Nejvíce případů bylo v Moravskoslezském kraji – 8 365 (-1 534), nejméně v Karlovarském kraji – 1 002 (-252).

Radiační nehoda vznikla 13. 7. 2012 v Mydlovarech, okr. České Budějovice. Na volné ploše firmy DIAMO s. p. byl nalezen radioaktivní materiál - zkorodované železné koule (cca 40kg). Naměřené hodnoty dávkového příkonu nebyly bezprostředně zdraví ohrožující. Jednotka PO, zástupci SÚJB a firma DIAMO s. p. nález zajistili pro konečnou likvidaci.

Plané poplachy oproti stejnému období roku 2011 o 2 % poklesly, přičemž jejich podíl na celkovém počtu událostí také poklesl a činí 7,6 %. Nejčetnější jsou plané poplachy způsobené elektrickou požární signalizací (44,6 %), další plané poplachy jsou způsobeny přivoláním k případu, který měl příznak požáru (22,6 %), zneužití jednotky PO (5,6 %), přivolání k nenahlášenému pálení (10,3 %) a z jiných důvodů (16,9 %). Nejvíce planých poplachů bylo ve Středočeském kraji – 1 011 (+1), nejméně v kraji Libereckém – 169 (+1).

Jednotky PO bezprostředně zachránily nebo evakuovaly z ohrožených prostor za období leden – září letošního roku 58 911 (+25 511) osob - nejvíce při technických pomocích, požárech, dopravních nehodách.

Zároveň bylo 365 hasičů zraněno (+32), z toho 265 profesionálních (+13) a 100 dobrovolných (+19). Při likvidaci požáru porostu trávy zemřel dne 26. 8. 2012 dobrovolný hasič - člen SDH Lomnice, okr. Sokolov Při zásazích se vyskytlo také 1 683 (+103) usmrcených osob - jednotky PO pomáhaly při jejich vyprošťování a vynášení při dopravních nehodách, požárech a při nouzovém otevírání bytů. Dále byla 13 769 (+1 759) zraněným osobám poskytnuta předlékařská pomoc (převážně u dopravních nehod, technických pomocí a požárů).

Rozhodující podíl na spolupráci při zásahu u událostí s jednotkami PO má Policie ČR a zdravotnická záchranná služba. Tyto 3 složky jsou hlavními garanty integrovaného záchranného systému. Za období leden až září 2011 bylo evidováno 74 704 (+ 9 %) případů součinnosti jednotek PO s ostatními složkami IZS, přičemž nejvíce – 60,0 % z celkového počtu připadlo na Policii ČR, na zdravotnickou záchrannou službu – 21,0 % a na obecní policii 9,9 %. Zbytek tvoří pomoci zejména pohotovostních služeb, místních služeb, firem, institucí, obecních zastupitelstev a dalších.

Požáry - základní ukazatele v období leden - září

Rok	Počet požárů	Škoda mil. Kč	U	Z
2010	13 851	1 452,9	82	780
2011	16 499	1 806,5	94	826
2012	16 793	1 999,9	101	962

U - počet usmrcených osob, Z - počet zraněných osob

V období od 1. ledna do 30. září 2012 vzniklo v ČR 16 793 požárů s účastí i bez účasti jednotek PO (+294). Přímé škody dosáhly částky 1 999,9 mil. Kč (+193,4). Při požárech bylo 101 osob usmrceno (+7) a dalších 962 osob bylo zraněno (+136). Jednotky PO uchránily před zničením hodnoty ve výši 8,2 mld. Kč (+3,0). Počet požárů je oproti stejnému období roku 2011 vyšší o 1,8 %, přímé škody jsou vyšší o 10,7 %, počet usmrcených je vyšší o 7,4 %, počet zraněných vyšší o 16,5 %. Nejvíce požárů vzniklo v březnu – 19,7 % z celkového počtu, nejméně naopak v září – 7,8 %. Výši škod ovlivnily velké požáry (se škodou 1 mil. Kč a vyšší), kterých vzniklo loni 291(+24), přímé škody u nich dosáhly více než 69 % z celkových škod.

Přehled připravovaných velkých cvičení pro léta 2013 a 2014

2013

ZÓNA 2013

- Cvičení orgánů krizového řízení vybraných ústředních správních úřadů (ÚSÚ), kraje Vysočina a Jihomoravského kraje.
- Tématem je činnost ÚSÚ, složek IZS a dalších subjektů při řešení událostí vzniklých v souvislosti s radiační havárií na jaderné elektrárně Dukovany.
- Cvičení připravuje MV-GŘ HZS ČR ve spolupráci s SÚJB a MO. Za cvičení odpovídá ministr vnitra.
- Účastní se: Ústřední krizový štáb v čele s ministrem vnitra, krizový štáb SÚJB a krizové štáby vybraných ÚSÚ, kraje Vysočina a Jihomoravského kraje, ČEZ a.s., vybrané složky IZS a vyčleněné síly a prostředky AČR.
- Datum provedení: březen 2013.

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 státu, 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. 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 zvládání 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:
Kauza metylalkohol v České republice

Počátek kauzy otrav metylalkoholem v České republice je možné datovat na den **3. září 2012, kdy bylo zaznamenáno první úmrtí ženy a muže z Havířova** (Moravskoslezský kraj), ačkoliv pozdějšími šetřeními (na základě výsledků ze 155 pitev zemřelých v Moravsko-slezském kraji, které patologové zpětně prověřili ke dni 14. září 2012) byl první případ úmrtí na otravu metylalkoholem datován již na 13. května 2012.

Prvotním podnětem k činnosti státních orgánů byla právě úmrtí v Moravskoslezském kraji, která však z počátku nenasvědčovala, že by se jednalo o rozsáhlejší případ intoxikací methylalkoholem. Postupně však s přibývajícími případy získávala celá kauza na vážnosti a také do ní byla čím dál víc zainteresována média i široká veřejnost. Dne 12. září 2012 také zasedali ve všech krajích na operativních poradách zástupci jednotlivých dotčených složek a organizací včetně zástupců krajských hygienických stanic.

Průběh celé kauzy je z médií poměrně dobře znám, na tomto místě bude nicméně, již po opadnutí vlny veřejného zájmu, možné učinit určité shrnutí. Na základě údajů od Policie České republiky a dalších oficiálních zdrojů včetně zdrojů veřejně dostupných je **na území státu v souvislosti s kauzou „Metanol“ v období od 1. 9. 2012 do 17. ledna 2013 evidováno celkem 124 poškozených osob včetně osob ze Slovenska, z toho 66 bylo hospitalizovaných či jen ošetřených a 40 mrtvých**. Poslední úmrtí bylo evidováno ve středu 9. ledna 2013 v Olomouckém kraji, kdy došlo k potvrzení ze strany Soudního lékařství v Olomouci o úmrtí muže středního věku, který se dne 7. ledna 2013 otrávil methylalkoholem. V rámci dosud provedených úkonů trestního řízení bylo Policií České republiky **zajištěno okolo 4 000 vzorků kontaminovaného alkoholu a zhruba 6 000 litrů čistého metylalkoholu**. Dále byla zajištěna stáčecí zařízení a zjištěna místa distribuce a více jak 15.000 litrů dalších podezřelých tekutin.

Mezi hlavní činnosti, které zajišťoval Hasičský záchranný sbor České republiky zejména ve spolupráci s Policií ČR a Celní správou České republiky patřila urgentní analýza dodaných vzorků prováděná v chemických laboratořích Hasičského záchranného sboru České republiky a servisní úlohy jednotek Hasičských záchranných sborů krajů spočívající v práci s těžkou manipulační technikou (kontejnery o objemu tisíc litrů), v přepravě zabavených zásob do skladů, v uskladnění části zabavených zásob na žádost Policii České republiky ve skladech Hasičského záchranného sboru České republiky). Doposud Hasičský záchranný sboru České republiky přijal více jak 2.000 vzorků, z nichž bylo více jak 200 pozitivních. Hasičský záchranný sboru České republiky nadále pro Policii České republiky nebo Celní správu České republiky provádí testy v laboratořích.

Celkem je v souvislosti s kauzou methanol **vedeno vyšetřování proti více než 60 obviněným osobám, z nichž u více jak 10 osob probíhá vyšetřování vazebně**. Je však nezbytné doplnit, že v rámci vedeného vyšetřování dochází k neustálé změně stavu jednotlivých trestních řízení. Ke změnám dochází jak v počtu trestních řízení, kdy dochází ke slučování věcí k hlavnímu trestnímu řízení, které je vedeno pod Krajským ředitelstvím Policie Zlínského kraje, tak v počtu osob obviněných, zemřelých, vazebně trestně stíhaných, tak i dalších skutečností, které jsou ze zřejmých důvodů s ohledem na vyšetřování ze strany Policie ČR buď zveřejněny v omezeném rozsahu nebo nezveřejněny.

Vybrané události ve sledovaném období

Září

Zřízení nového Centra krizového řízení v Jihočeském kraji

Rychlejší reakci na mimořádné události, jako jsou například živelné pohromy, umožní Jihočeskému kraji nové Centrum krizového řízení. Zřízení centra si vyžádalo celkovou investici ve výši pěti miliónů korun, která byla plně uhrazena z prostředků společnosti ČEZ na základě takzvané rámcové smlouvy o spolupráci uzavřené mezi společností ČEZ a Jihočeským krajem v dubnu 2009 na dobu deseti let. Rámcová smlouva vyčleňuje podle uzavřených dohod zdroje na podporu rozvoje infrastruktury v regionu v už zmíněném desetiletém období ve výši 3,7 miliardy korun.

Centrum se stane významnou součástí zabezpečení krizového řízení v Jihočeském kraji především při řešení mimořádných událostí velkého rozsahu a krizových situací ohrožujících životy, zdraví a majetky občanů, kdy je aktivován krizový štáb kraje. Na základě rámcové smlouvy se společnost ČEZ zavázala vyplatit v letech 2009 až 2018 na podporu složek IZS v Jihočeském kraji celkem 100 milionů korun. V letech 2010 až 2012 už byly provedeny či ještě budou dokončeny akce za bezmála 44 milionů korun. Šlo mimo jiné o nákup techniky pro Zdravotnickou záchrannou službu Jihočeského kraje, Policii ČR, Hasičský záchranný sbor, Český červený kříž atd.

Součástí projektu bylo nejen vybudování Centra krizového řízení, ale také nákup vozidla Škoda Octavia Scout pro potřeby práce v terénu a přenosu informací a obrazu z postiženého území prostřednictvím videokonference do centra k využití členům krizového štábu kraje. Potřeba nových prostor pro činnost stálé pracovní skupiny krizového štábu vyvstala po zkušenostech při řešení krizových situací v minulých letech, jako byly například povodně v letech 2006, 2009, společných cvičení Zóna 2007 a 2010 (teoretická simulovaná havárie v elektrárně Temelín), nebo s KVS BIO 2010 (veterinární cvičení slintavka-kulhavka). Centrum krizového řízení nahradí svým způsobem provizorní prostory v Presscentru krajského úřadu, které se při vzniku krizové situace musely vybavit potřebnou technikou a dokumentací.

Bezpečnostní cvičení Horizont 2012

Ve dnech 4. – 6. září 2012 proběhlo mezinárodní cvičení složek Integrovaného záchranného systému (IZS) v prostorách elektrické stanice ČEPS. Cvičení HORIZONT 2012 se uskutečnilo pod záštitou ministra vnitra ČR, ministra průmyslu a obchodu ČR a ministerstva hospodářství SR. Ústředním námětem cvičení byl simulovaný útok na významné prvky energetické kritické infrastruktury na území ČR a SR. Další informace o cvičení viz první kapitola této zprávy, věnující se energetické bezpečnosti.

Cvičení IZS „Humanitární pomoc 2012“ v Pardubickém kraji

Pardubický kraj společně s hasiči uskutečnil ve dnech 20. – 21. září 2012 další taktické cvičení složek integrovaného záchranného systému. To bylo zaměřené na zajištění nouzového přežití v případě povodní a hasiči společně s dalšími organizacemi si při něm vyzkouší stavbu a provoz materiální základny humanitární pomoci (MZHP). MZHP je doplňujícím prvkem integrovaného záchranného systému při poskytování pomoci za mimořádných situací. Je předurčena k zabezpečení základních životních potřeb (ubytování, přípravy a výdej stravy, ošacení) postiženému obyvatelstvu, a to na dobu nezbytně nutnou. Na cvičení došlo k vybudování MZHP v prostoru letiště Polička.

Materiál pro výstavbu základny byl do prostoru letiště přepraven ze skutečského skladu Základny logistiky Olomouc. Cílem taktického cvičení bylo prověření součinnosti složek IZS, orgánů

krizového řízení a dalších spolupracujících subjektů při výstavbě a provozu MZHP na území Pardubického kraje a prověření připravenosti jednotek SDH obcí předurčených k plnění speciálních úkolů v ochraně obyvatelstva a vybraných humanitárních jednotek Českého červeného kříže.

Říjen

Cvičení záchrany zraněného ze stožáru vysokého napětí

Nedaleko obce Mošnov na Teplicku se 15. října konalo společné cvičení složek integrovaného záchranného systému s názvem „LETKA 2012“. Ústředním motivem byla záchrana zraněné osoby, která zůstala po úrazu elektrickým proudem nehybně viset na stožáru velmi vysokého napětí.

Na cvičení se podílelo více než 70 záchranářů, příslušníků Hasičského záchranného sboru, Letecké záchranné služby, Policie ČR a Horské služby Ústeckého kraje. Od dopoledních hodin společně opakovaně nacvičovali záchranné práce nejen z vrtulníku záchranné letecké služby, ale také přímo na stožáru ve výšce přibližně 18 metrů nad zemí. Jednou z nejobtížnějších fází cvičení byl letecký manévr vrtulníku letecké záchranné služby v blízkosti vodičů.

S ohledem na povětrnostní podmínky a práce ve výškách bylo cvičení velmi náročné i na fyzickou připravenost všech záchranářů. Cílem cvičení bylo ověřit komunikační kanály a celkovou koordinaci mezi společností ČEPS a všemi složkami integrovaného záchranného systému.

Cvičení záchranářů v rozvodně Kočín

V úterý 9. října těsně před čtrnáctou hodinou zachytily kouřové detektory dým v areálu rozvodny Kočín. Jednalo se o další z řady společných cvičení firmy ČEPS se složkami integrovaného záchranného systému, tentokrát pod názvem „KOČÍN 2012“.

Po ověření signálu z detektorů byl do rozvodny přivolán Hasičský záchranný sbor, byl vyhlášen požární poplach a proběhla úplná evakuace. Pracovník provozní směny ČEPS kontaktoval Policii ČR, která v případě potřeby zajišťuje evakuaci specialistů společnosti ČEPS z rozvodny do náhradní lokality v Hradci u Kadaně.

V objektu rozvodny uvízla jedna osoba, která se nadýchala zplodin. To si vyžádalo okamžitý zásah hasičské jednotky. Oheň však hasičům zatarasil přístupovou cestu, a tak se figurant dočkal vyproštění až pomocí výsuvného žebříku. Cvičení prověřilo nejen tradičně dobrou připravenost jednotlivých složek integrovaného záchranného systému na nejrozmanitější krizové situace, ale i funkčnost všech vzájemných komunikačních kanálů.

Proběhlo evropské cvičení Multi Layer 2012

Ve dnech 1. až 26. října 2012 se pod označením Multi Layer 2012 konalo cvičení orgánů krizového řízení Evropské unie. Cílem cvičení bylo prověřit činnost těchto orgánů při plánování vojenské operace a civilní mise společné bezpečnostní a obranné politiky EU. Modelová operace, která proběhla ve cvičném geopolitickém prostředí v oblasti severovýchodní Afriky, byla zaměřena na řešení krizové situace ve fiktivním státu Nusia a v několika jeho sousedních zemích vzdálených šest tisíc kilometrů od Evropy. Plánovaná vojenská operace a civilní mise zahrnovala prvky, jako jsou odzbrojení, demobilizace a začlenění do společnosti, humanitární činnost a akce proti pirátství. Jedná se o pravidelné cvičení, při kterém nedošlo k žádnému skutečnému nasazení vojsk.

V rámci České republiky cvičení proběhlo na pracovištích orgánů krizového řízení pod vedením prvního náměstka ministra obrany Vlastimila Picka. Cvičení představuje konkrétní formu plnění závazku státu vůči Evropské unii v oblasti vytváření a udržování mezinárodní bezpečnosti.

Listopad

Cvičení CMX a Cyber Coalition 2012

Cvičení orgánů krizového řízení NATO Crisis Management Exercise 2012 bylo zaměřeno na prověření aliančních postupů krizového řízení, na plánování a rozhodování na strategické politicko vojenské úrovni. Cvičení CMX bylo v roce 2012 propojeno se souběžně probíhajícím cvičením kybernetické obrany Cyber Coalition 2012, které bylo zaměřeno na řešení krizové situace vzniklé v důsledku kybernetických útoků na informační a komunikační systémy NATO a na kritickou infrastrukturu některých členských zemí Aliance.
Cvičný scénář byl postaven na řešení složité mezinárodní krizové situace, která vznikla v důsledku dlouhotrvajících konfliktů mezi dvěma fiktivními ostrovními státy v Indickém oceánu, a v důsledku ohrožení některých členských států Severoatlantické aliance agresivními aktivitami dvou nepřátelských zemí. Modelová situace zahrnovala stupňující se hrozbu chemických, biologických a radiačních útoků a široký rozsah kybernetických útoků.
Cvičení CMX se mimo zemí NATO zúčastnily z důvodu zeměpisné blízkosti některým událostem scénáře i dva partnerské státy Aliance, Finsko a Švédsko. Oba státy se spolu s Rakouskem zapojily i do cvičení Cyber Coalition.

Mise Mezinárodní agentury pro atomovou energii označila Temelín za bezpečný

V listopadu proběhla v Temelíně prověrka, ve které mezinárodní experti označili provoz elektrárny za bezpečný a probíhající v souladu s kritérii MAAE. Tzv. mise OSART přijela na základě požadavku české vlády a byla to v pořadí již 26. mezinárodní kontrola, kterou Temelín bezpečně prošel.

Prosinec

Cvičení v oblasti bezpečnosti civilního letectví „Terminál 2012“

V souladu s úkolem z Národního plánu pro řešení protiprávních činů v civilním letectví se 12. prosince 2012 uskutečnilo na pracovišti Ústředního krizového štábu MV cvičení orgánů zodpovědných za bezpečnost civilního letectví pod názvem „Terminál 2012“. Cvičení, jehož tématem bylo řešení vybraných mimořádných událostí ohrožujících bezpečnost civilního letectví, organizoval odbor bezpečnostní politiky Ministerstva vnitra.
Akce se zúčastnili zástupci celkem šestnácti institucí, jak z řad státní správy, bezpečnostních a zpravodajských složek, tak i ze soukromého sektoru (např. zástupci Letiště Praha). V rámci cvičení bylo postupně diskutováno pět rozpracovaných scénářů, které spojovalo téma narušení bezpečnosti civilního letectví, a které byly předem prodiskutovány s jednotlivými bezpečnostními složkami tak, aby zachycovaly reálné hrozby a pomohly ukázat připravenost České republiky těmto hrozbám čelit. Hlavním cílem cvičení bylo identifikovat nedostatky v přípravě a koordinaci, které by se mohly projevit během reakce na skutečnou mimořádnou událost, a navrhnout možná zlepšení.

Záchranářům na Šumavě bude i nadále pomáhat horská služba

Nové smlouvy o spolupráci podepsali v Plzni a Českých Budějovicích zástupci Horské služby a zdravotnickými záchrannými službami (ZZS) obou regionů.
"Poprvé se v takovém dokumentu objevuje existence tzv. first respondera, tedy záchranáře mimo ZZS, který má ovšem adekvátní výcvik a vzdělání," uvedl Michal Janďura, náčelník Horské služby Šumava. Dodal, že Horská služba spolupracuje s oběma krajskými záchrankami již řadu let při zásazích v terénu i při společných cvičeních a školících akcích. Horští záchranáři poskytují první předlékařskou první pomoc zejména v místech, kam se nemá v zimních, ale i v letních měsících technika zdravotníků šanci dostat.

NOVINKY V LEGISLATIVĚ ČR ZA SLEDOVANÉ OBDOBÍ

Energetika a energetická bezpečnost

Předpis 498/2012 Sb.**,** kterým se mění zákon č. 44/1988 Sb.**, o ochraně a využití nerostného bohatství (horní zákon)**, ve znění pozdějších předpisů.
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=79238&src=nove&rpp=15#local-content

Předpis 478/2012 Sb. **o vykazování a evidenci elektřiny a tepla z podporovaných zdrojů**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=79182&src=nove&rpp=100#local-content

Předpis 477/2012 Sb. **o stanovení druhů a parametrů podporovaných obnovitelných zdrojů**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=79181&src=nove&rpp=100#local-content

Předpis 445/2012 Sb., **změna vyhlášky o udělování licencí pro podnikání v energetice**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78771&src=nove&rpp=100#local-content

Předpis 440/2012 Sb., **o zárukách původu elektřiny z obnovitelných zdrojů energie**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78735&src=nove&rpp=100#local-content

Předpis 438/2012 Sb., **změna vyhlášky o pravidlech trhu s elektřinou**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78733&src=nove&rpp=100#local-content

Předpis 436/2012 Sb., **změna vyhlášky o pravidlech trhu s plynem**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78638&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Předpis 429/2012 Sb., **změna nařízení o dotacích na podporu elektřiny z obnovitelných zdrojů**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78583&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Předpis 387/2012 Sb., **o státní autorizaci na výstavbu výrobny elektřiny**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78536&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Předpis 383/2012 Sb., **o podmínkách obchodování s povolenkami na emise skleníkových plynů**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78497&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Předpis 355/2012 Sb., **o dotacích z rozpočtu na podporu elektřiny z obnovitelných zdrojů**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78417&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Předpis 348/2012 Sb., **změna vyhlášky o způsobu regulace cen v energetice**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78381&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Bezpečnost finančních institucí

Předpis 413/2012 Sb., **změna vyhlášky o předkládání informací ČNB finančními institucemi**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78573&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Předpis 372/2012 Sb., **změna vyhlášky o žádostech povolení některých činností na finančním trhu**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78476&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Informační technologie a kyberbezpečnost

Předpis 357/2012 Sb., **o uchovávání, předávání a likvidaci provozních a lokalizačních údajů**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78419&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Krizové řízení

Předpis 394/2012 Sb.**, změna vyhlášky o provádění hospodářských opatření pro krizové stavy**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78543&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Předpis 389/2012 Sb.**, změna vyhlášky o radiační ochraně**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78538&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Předpis 385/2012 Sb.**, změna zákona o zdravotnické záchranné službě**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78499&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Předpis 379/2012 Sb.**, změna vyhlášky o báňské záchranné službě**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78493&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Předpis 344/2012 Sb., **o stavu nouze v plynárenství a o bezpečnostním standardu dodávky plynu**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78377&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Předpis 307/2012 Sb., **o místní a časové dostupnosti zdravotních služeb**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78241&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Předpis 306/2012 Sb., **o podmínkách předcházení vzniku a šíření infekčních nemocí**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78240&fulltext=&nr=&part=&name=2012&rpp=15#local-content

Předpis 296/2012 Sb., **o požadavcích na vybavení zdravotnické dopravní služby**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=78192&fulltext=&nr=&part=&name=2012&rpp=15#local-content

KONFERENCE A SETKÁNÍ

Připravované akce v ČR a v SR v příštím roce

Energetika a energetická bezpečnost

26. – 27. 2. 2013	Asociace energetických manažerů **Evropské trhy s energií do roku 2020. Vliv dotací a regulace na ceny energie** Hotel Olympik, Praha http://aem.cz/planovane-akce
5. – 6. 3. 2013	Business Forum **13. Energetický kongres ČR** Hotel Marriot, Praha http://www.business-forum.cz/13-energeticky-kongres-cr/o-kongresu.html
6. 3. 2013	Společnost konference Brno **Očekávaný vývoj odvětví energetiky v ČR a na Slovensku** Brno, pozvánka : http://konference.org/energetika2012/
11. – 12. 4. 2013	Magazín PRO-ENERGY **PRO-ENERGY FÓRUM 2013** Hotel Patria, Štrbské Pleso, Slovensko http://www.pro-energy.cz/konference/article?pos_id=70
16. – 17. 4. 2013	**Top Gas 2013 – bezpečný provoz plynovodů** NH Prague http://www.konference.cz/akce/detail-2723-Bezpecny-provoz-plynovodu/
23. – 24. 4. 2013	**Plynárenství ČR a SR 2013** Regulace a legislativa, plynárenský trh ve střední Evropě NH Prague http://www.konference.cz/akce/detail-2719-Plynarenstvi-CR-&-SR-2013/

Bezpečnost finančních institucí

8. 2. 2013	Bankovní institut vysoká škola, Praha **Bezpečnost firmy a podnikání, Mezinárodní vědecká konference** nutnost vyplnění přihlášky: http://www.bivs.cz/novinky/novinky/mezinarodni-vdecka-konference-bezpenost-firmy-a-podnikani
26. – 27. 2. 2013	**Evropský platební styk 2013** Přelomové novinky v platebním styku a nástrojích. NH Prague http://www.konference.cz/akce/detail-2701-Evropsky-platebni-styk-2013/

7. – 10. 3. 2013 **Peníze 2013**
Veletrh osobních financí a osobních investičních příležitostí
Brno, Výstaviště
http://www.bvv.cz/penize/

10. – 11. 4. 2013 **6 účinných nástrojů prevence a detekce podvodů**
Zabránění podvodům především v organizacích ve finančním sektoru.
Praha
http://www.business-continuity.cz/cc-21-6-ucinnych-nastroju-prevence-a-detekce-podvodu-zkusenosti-z-praxe.php

14. – 15. 5. 2013 **White Colar Crime**
Podvody bílých límečků, finanční kriminalita, právní aspekty a praktické zkušenosti s prevencí, detekcí a vyšetřováním.
Praha, místo bude upřesněno
http://www.business-continuity.cz/ss-25-rizeni-rizika-podvodu.php

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-vysetrovani-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

19. 3. 2013 **IT Security Workshop** (možnosti v oblasti ochrany dat)
Praha, pozvánka:
http://www.itsw.cz/

8. – 9. 4. 2013 **Internet ve státní správě a samosprávě**
Kongresové centrum Aldis, Hradec Králové
Registrace na:
https://www.isss.cz/portal/login.asp?req=%2Fportal%2Findex%2Easp&empty=1

16. 4. 2013 **Business Intelligence Conference**
Business Intelligence aplikace umožňují řídícím pracovníkům získat relevantní informace pro rozhodovací proces díky výkonným analytickým a vykazovacím nástrojům. Konference se věnuje tématům: Business Intelligence, datové sklady, OLAP, dolování dat, systémy pro podporu rozhodování.
Kongresové centrum U Hájků, Praha
http://www.bicon.cz/

14. 5. 2013 **Bezpečnost v Cloudu**
Konference se bude soustředit na bezpečnostní témata v Cloud Computingu.

Kongresové centrum U Hájků, Praha
www.bezpecnostvcloudu.cz

25. 4. 2013 **Security Fórum 2013**
Agenda: kyberútoky, mobilní zařízení, spam, moderní firewally.
http://www.konferenceit.cz/html/kalendar-konferenci-a-akci-2013.html

28. 5. 2013
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.
Hotel Crown Plaza Bratislava (1. termín)
Kongresové centrum U Hájků, Praha (2. termín)
http://ccc.exponet.sk/
http://www.cloudconference.cz/

29. – 30. 5. 2013 Časopis RSM
Mezinárodní konference o informační bezpečnosti
Praha, Pozvánka:
http://www.cabm.cz/uploads/cabm.cz/IS2-2013-CfP-cz-mail.pdf

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/

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 přehlídku 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

29. – 30. 1. 2013 Vysoká škola Báňská a Sdružení požárního a bezpečnostního inženýrství
Ochrana obyvatelstva – DEKONTAM 2013
Ostrava, pozvánka:
http://www.skpz.cz/wp-content/uploads/2012/11/pozv%C3%A1nka-OOb-Dekontam-2013.pdf

7. – 8. 2. 2013	Úrazová nemocnice v Brně s Lékařskou fakultou Ostravské univerzity Ostrava **VIII. mezinárodní kongres Medicína katastrof Brno 2013** Hlavními tématy tohoto ročníku budou: hromadné postižení zdraví, bezpečnost nemocnic (hrozba bombou), spolupráce IZS. V rámci kongresu proběhne workshop „Příprava traumaplánů“. Hotel Holiday Inn, Brno http://www.meka-brno.cz/
19. 4. 2013	Centrum pro bezpečnostní a strategická studia **VI. Studentská konference k aktuálním bezpečnostním tématům** FSS MU Brno, registrace: http://www.cbss.cz/konference/call-for-papers-studentska-konference-bezpecnost-v-dobe-neklidu/
24. 4. 2013	Vysoká škola báňská – Technická univerzita Ostrava **Požární bezpečnost stavebních objektů** Posluchárna Fakulty bezpečnostního inženýrství http://www.vsb.cz/info/?&lang=cs&block=simple&reportId=15946&showExpired=true&showExpired=true
2. – 4. 5. 2013	**FIRECO 2013** 11. mezinárodní výstava hasičské, záchranářské a zabezpečovací techniky. Výstaviště Trenčín, Slovensko http://www.expocenter.sk/
22. – 24. 5. 2013	**Mezinárodní veletrh obranné a bezpečnostní techniky (IDET)** Jeho součástí je mezinárodní konference CATE, jejímž tématem je Společnost – Armáda – Technika – Životní prostředí. Souběžně na výstavišti probíhá výstava **ISET/PYROS požární a bezpečnostní techniky**. http://www.bvv.cz/idet/
22. – 24. 5. 2013	**Bezpečnost a ochrana utajovaných informací** (jednacím jazykem je angličtina, ale zajištěn simultánní překlad) Brno, registrace : http://spi.unob.cz/registrace1.asp
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 záchranáři** 12. ročník akce představující Integrovaný záchranný systém. Výstava moderní policejní a požární techniky. Lysá nad Labem, areál výstaviště http://www.vll.cz/veletrh-146
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. 1. 2013 **ENERTEC**
Mezinárodní odborný veletrh energie
Lipsko, Německo
http://www.enertec-leipzig.de/

5. – 6. 3. 2013 **Russia Power**
Mezinárodní veletrh energetiky
Moskva, Rusko
http://www.russia-power.org/en_GB/index.html

5. – 8. 5. 2013 **WINDPOWER**
Výstava a konference na téma větrné energie
Chicago, USA
http://www.windpowerexpo.org/

6. – 8. 5. 2013 **Power Gen India & Central Asia**
Mezinárodní veletrh energetiky
Bombaj, Indie
http://www.veletrhyavystavy.cz/cz/veletrh-vystava/15709-power-gen-india-central-asia/

14. – 16. 5. 2013 **EXPOPOWER**
Mezinárodní veletrh energetiky
Poznaň, Polsko
http://www.expopower.pl/pl/

18. – 20. 6. 2013 **PCIM CHINA**
Mezinárodní výstava a konference na téma elektrické energie
Šanghaj, Čína
http://www.pcim-china.com/

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

Bankovnictví a finanční bezpečnost

6. – 8. 4. 2013 **FORINVEST**
6. mezinárodní veletrh finančních služeb, investic, pojištění a bankovního sektoru
Valencie, Španělsko
http://www.spanelske-veletrhy.cz/

24. – 25. 2. 2013 **4, International Conference on Financial Theory and Engineering (ICFTE)**
Mezinárodní finanční konference
Řím, Itálie
http://www.icfte.org/

Informační technologie a kyberbezpečnost

18. – 20. 2. 2013 **IV. mezinárodní konference a odborný veletrh IT řešení pro veřejnou přepravu osob**
Součástí veletrhu bude bezpečnostní konference, jejímž tématem bude kromě řešení a strategie k aktuálním informačním technologiím ve veřejné osobní dopravě také obrana dopravních technologií před teroristy.
Výstaviště Karlsruhe
www.it-trans.org

4. – 6. 3. 2013 **CyberSec2013**
The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic; Malajsie
http://sdiwc.net/conferences/2013/Malaysia3/

12. – 15. 3. 2013 **Black Hat Europe**
Konference o kybernetické bezpečnosti a fenoménu hackingu
Grand Hotel Krasnapolsky, Amsterdam, Nizozemsko
http://www.blackhat.com/eu-13/

13. – 16. 4. 2013 **HKTDC International ICT Expo**
Mezinárodní výstava informačních technologií
Hongkong, Čína
http://www.hktdc.com/fair/ictexpo-en

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

20. – 21. 2. 2013 **FeuerTRUTZ**
Odborný veletrh protipožární prevence
Norimberk, Německo
http://www.feuertrutz.de/

9. – 12. 4. 2013 **LAAD 2013**
Mezinárodní výstava obrany a bezpečnosti, včetně vybavení pro vojenské i policejní složky.
Rio de Janeiro, Brazílie
http://laadexpo.com.br/english/

10. – 12. 4. 2013 **ISC WEST 2013**
Mezinárodní výstava a konference o veřejné bezpečnosti, biometrice, požární ochraně a dalších bezpečnostních tématech.
Las Vegas, USA
http://www.iscwest.com/

14. – 16. 4. 2013 **ASIS International 12th European Security Conference & Exhibition**
Konference týkající se hodnocení hrozeb, krizového řízení, bezpečnosti kyberprostoru a široké škály bezpečnostních témat.
Gothenburg, Švédsko
http://www.asisonline.org/education/programs/gothenburg/default.htm

24. – 25. 4. 2013 **Counter Terror Expo**
Součástí této výstavy bude konference, která se bude týkat témat jako globální boj proti terorismu, národní kritická infrastruktura – ochrana, bezpečnost, odolnost; bezpečnost kyberprostoru a elektronický terorismus, ochrana rušných míst.
Olympia, Londýn
http://www.counterterrorexpo.com/page.cfm/link=2

červen 2013 **Total Counter Terrorism Summit**
Konference týkající se konkrétních taktik a strategií prevence terorismu, ale i reakcím na teroristické akce. Přesné datum a místo konání akce ještě není stanoveno.
Velká Británie
http://www.clocate.com/conference/TOTAL-Counter-Terrorism-Summit-2013/27697/

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.htmv

Zdroje použité pro monitoring

MV, PČR, MV-GŘ HZS ČR, MPO, MO, MZV, ČTK, vlada.cz, ceps.cz, cez.cz, mero.cz, pressweb.cz, energetickakoncepce.cz, prumysl.cz, ČT 24, ČRo, net4gas.cz, cepsr.com, banktech.com, lidovky.cz, tpeb.cz, euraktiv.cz, europa.eu, ihned.cz, eset.cz, root.cz, computerworld.cz, itbiz.cz, mcaffee.com, krebsonsecurity.com, zachranny-kruh.cz, mayerbrown.com, isis-europe.eu, population-protection.eu, cad.cz, skpz.cz, bivs.cz, konference.org, novinky.cz, itsw.cz, isss.cz, forum2000.cz, bvv.cz, spi.unob.cz, cabm.cz, sdiwc.net, asisonline.org, counterterrorexpo.com, expopromoter.com, waset.org, iaem.com, it-trans.org, aem.cz, konference.ncbi.cz, ictsecurity.cz, khkjm.cz, muptimes.cz, ohk-most.cz, securiteknews.wordpress.com, cy2012.eu, eur-lex.europa.eu, csas.cz, denik.cz, csob.cz, root.cz, labs.nic.cz, govcert.cz, cesnet.cz, saferinternet.cz, bezpecnyinternet.cz, ceskenoviny.cz, zpravy.tiscali.cz, zdnet.com, net-security.org, radyvnouzi.cz, portal.gov.cz, konferenceit.cz, security-portal.cz, tyinternety.cz, cbss.cz, iir.cz, sbp.fsv.cuni.cz, vojenskaskola.cz, dspace.k.utb.cz, mup.cz, veletrhyavystavy.cz, blackhat.com, banksecurityportal.com, business-continuity.com, pro-energy.cz, energetika.cz, euroexpo.cz, europeum.org

Zdroje obrázky

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

Text neprošel jazykovou a stylistickou úpravou.