MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Situační zpráva
o vybraných oblastech bezpečnosti

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

za období 1. července do 31. prosince 2013

Odbor bezpečnostní politiky Ministerstva vnitra

leden 2014

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 cvičení RESTART 2014 a hlavním událostem a trendům v evropské energetice za sledované období.

V sekci o kybernetické bezpečnosti a informační kriminalitě čtenář nalezne oddíl zvlášť věnovaný mobilním hrozbám, kapitola zaměřená na bezpečnost finančních institucí pro změnu obsahuje exkurz o padělání platidel. Kapitola o krizovém řízení je rozšířena o přehled připravovaných velkých cvičení v roce 2014.

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 prvních třech čtvrtletích roku 2013. Z policejních statistik se zde dozvídáme, že celkový počet zaznamenaných trestných činů (325 366) meziročně vzrostl o 4%, nicméně stále zůstává pod průměrem posledních deseti let. K nárůstu docházelo zejména u krádeží vloupáním a u drogové kriminality, snížit se naopak podařilo počet loupeží a některých druhů dopravních nehod.

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 krádeže a podvody různého rozsahu. Vedle nich jsou to samozřejmě také nehody a mimořádné události, o kterých pojednávají statistiky Hasičského záchranného sboru. Mezi ty největší patřil červnový požár trafostanice v pražském Šeberově, se škodou převyšující 100 000 Kč.

Součástí této kapitoly je také shrnutí hlavních událostí a trendů v evropské energetice ve II. pololetí roku 2013. Naleznete zde shrnutí přípravy klimatických cílů Evropské unie do roku 2030, informace o proběhlém summitu V4 v Budapešti a přípravách jednotného evropského energetického trhu. Zvláštní oddíl je věnován velkému cvičení RESTART 2014, které bylo vůbec největší akcí tohoto druhu v energetice za poslední roky.

Kapitola o bezpečnosti finančních institucí v sekci věnované policejním statistikám upozorňuje mj. na nový trik pachatelů skimmingu, kterým se jim daří obcházet i nové formy zabezpečení bankomatů. Delší exkurz je věnován fenoménu padělání platidel. Podíváme se v něm na vývoj počtu zadržených padělků v několika posledních letech, zjistíme, jak zdatní jsou čeští padělatelé, a doporučíme několik základních tipů, jak poznat falešnou bankovku od pravé.

Další část zprávy se zabývá kybernetickou bezpečností a informační kriminalitou. Ta je jednou z nejrychleji se rozvíjejících forem kriminality – také v tomto roce zaznamenaly policejní statistiky nemalý nárůst trestné činnosti páchané s pomocí výpočetní techniky. Kromě tradiční sekce věnované aktivitám bezpečnostních složek a státní správy při boji s tímto fenoménem je delší exkurz věnován bezpečnosti mobilních zařízení. Kapitola také obsahuje varování před novým nebezpečným virem Cryptolocker.

Podstatná část kapitoly o krizovém řízení je věnována statistikám Hasičského záchranného sboru a jeho evidenci mimořádných událostí za rok 2013 (rozsáhlejší verzi těchto podkladů naleznete přímo na stránkách www.hzscr.cz). Obsažen je přehled největších požárů uplynulého roku a velkých cvičení, která jsou plánována v roce stávajícím. Zvláštní exkurzy blíže popisují cvičení Blaník 2013 a sérii cvičení k problematice aktivního střelce.

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

CELKOVÁ KRIMINALITA V ČR V ROCE 2013

Registrovaná kriminalita v meziročním srovnání

Za období od 1. 1. do 30. 9. 2013 Policie ČR registrovala celkem 325 366 trestných činů (+20 838, +6,8 %). I přes **poměrně vysoký nárůst** zůstala výše zjištěné kriminality **pod průměrem i mediánem posledních deseti let**. Řada analytiků dává nárůst počtu trestných činů také do spojitosti s lednovou amnestií prezidenta Václava Klause.

Zjištěná kriminalita celkem meziročně vzrostla o 6,8 %.

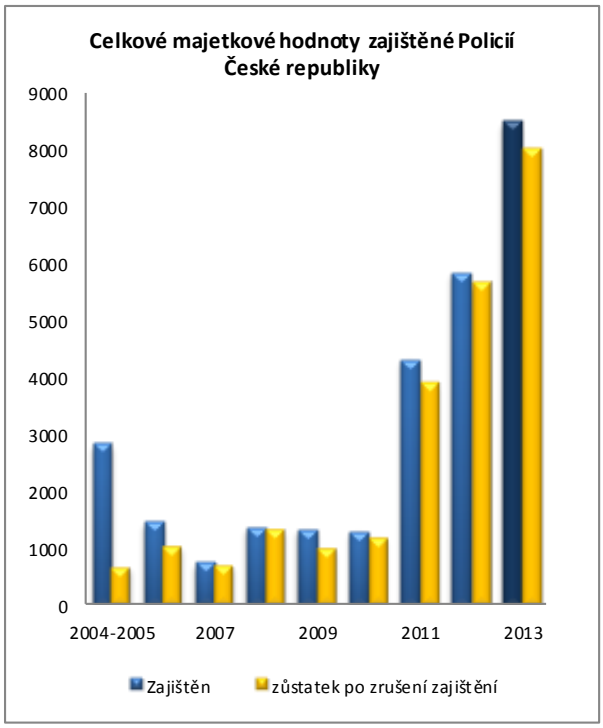
Počet objasněných trestných činů vzrostl o 7,5 %.

K nárůstu došlo u všech souhrnných kategorií policejní klasifikace kriminality:

- násilná kriminalita (+1,8 %)
- mravnostní kriminalita (+6,5 %)
- majetková kriminalita (+7,4 %)
- ostatní kriminalita (+11,7 %)
- zbývající kriminalita (+0,3 %)
- hospodářská kriminalita (+9,9 %)

Zjištěné škody poklesly o 15,1 %, zajištěné hodnoty vzrostly o cca 5,2 %.

Objasněno bylo 129 182 skutků (+9 014, +7,5 %). **Procentní nárůst počtu objasněných trestných činů byl vyšší než nárůst zjištěné kriminality.** Počet objasněných trestných činů byl nejvyšší od roku 2008 a na rozdíl od zjištěné kriminality hranici desetiletého průměru i mediánu překonal. Celková objasněnost dosáhla 39,7 %, což je **druhá nejvyšší hodnota za posledních deset let**, která znamená meziroční nárůst o 0,2 %.



Zjištěné hmotné škody meziročně **poklesly** o 15,1 % na cca **29,05 mld. Kč**

V oblasti zajišťování výnosů z trestné činnosti bylo v roce 2013 dosaženo (již potřetí) **dosud nejlepšího výsledku.**

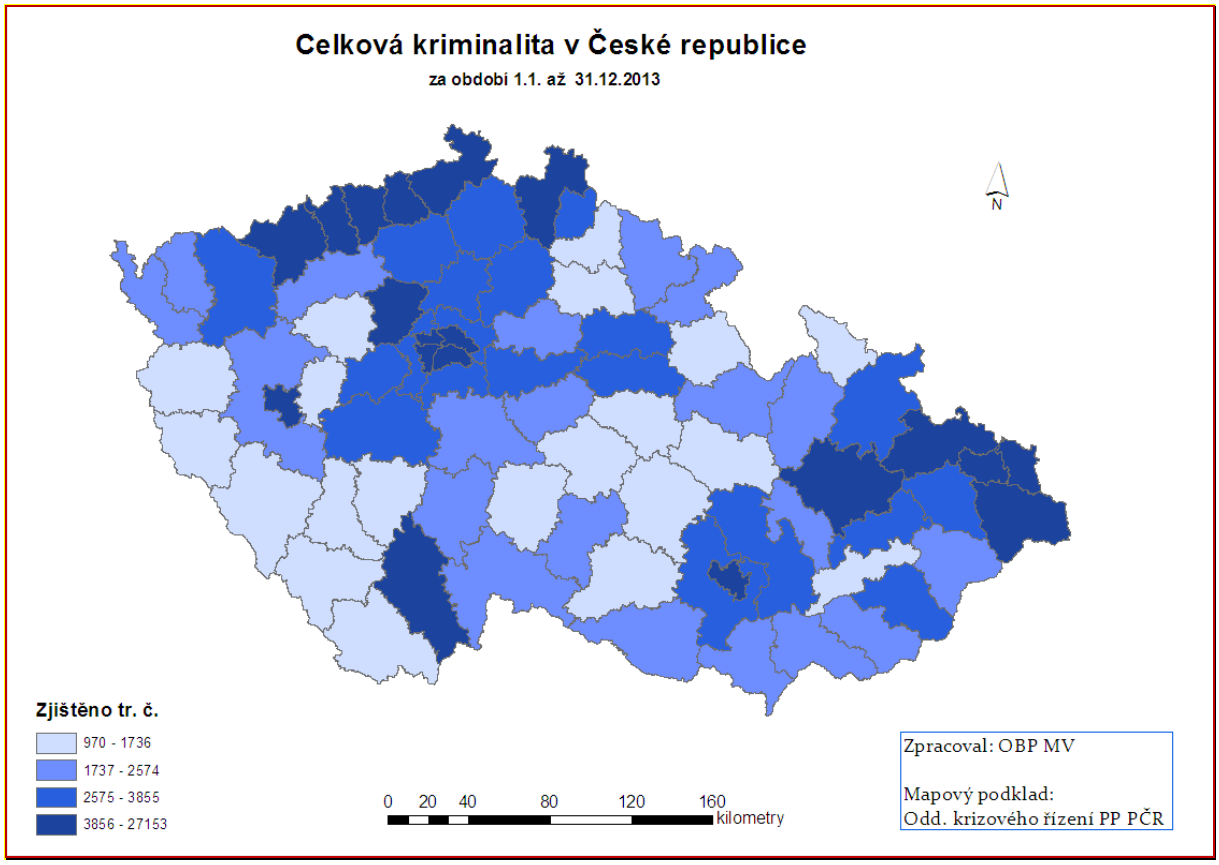
Nejvyšší škody byly způsobeny trestnými činy: krácení daně (6,8 mld.), podvod (3,9 mld.) a porušování povinností při správě cizího majetku (2,4 mld.). Při přepočtu způsobené škody na jeden případ připadá nejvyšší průměrná škoda právě na porušování povinností při správě cizího majetku (10,5 mil./skutek).[1]

Vybrané markanty registrované kriminality

Významně vzrostly **krádeže vloupáním** (do rodinných domů, obchodů atd.)

V absolutních číslech **nejvíce vzrostl počet krádeží vloupáním do ostatních objektů**[2] (+4 433, +13,6 %), jimiž také byly způsobeny škody přesahující částku 1,2 ml Kč. V roce 2013 bylo zjištěno 37 065 skutků, které byly takto v rámci takticko-statistické policejní klasifikace kvalifikovány. Jedná se tedy o nejčetnější trestnou činnost páchanou na území ČR, která irituje široké vrstvy občanů. Již dlouhodobý a strmý nárůst vykazuje **drogová kriminalita** …

V rámci násilné kriminality poklesl nejvíce počet **loupeží (-322)**. **Vysoký meziroční pokles** v absolutních číslech byl zaznamenán u trestného činu nedbalostní dopravní nehody (-483).



[1] Částky jsou zaokrouhleny.

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

Stíhané a vyšetřované osoby

V roce 2013 bylo celkem stíháno a vyšetřováno 117 682 osob. Meziroční vývoj je patrný z tabulky. Meziročně došlo k nárůstu počtu stíhaných a vyšetřovaných osob (+4 656 osob, + 4,1%).

Z tabulky vyplývá **razantní meziroční nárůst počtu recidivistů (+5 445, +9,6 %)**, který je již dlouhodobým trendem a nabývá na dynamice. Procentní nárůst počtu stíhaných a vyšetřovaných recidivistů překračuje procentní nárůst zjištěné trestné činnosti.

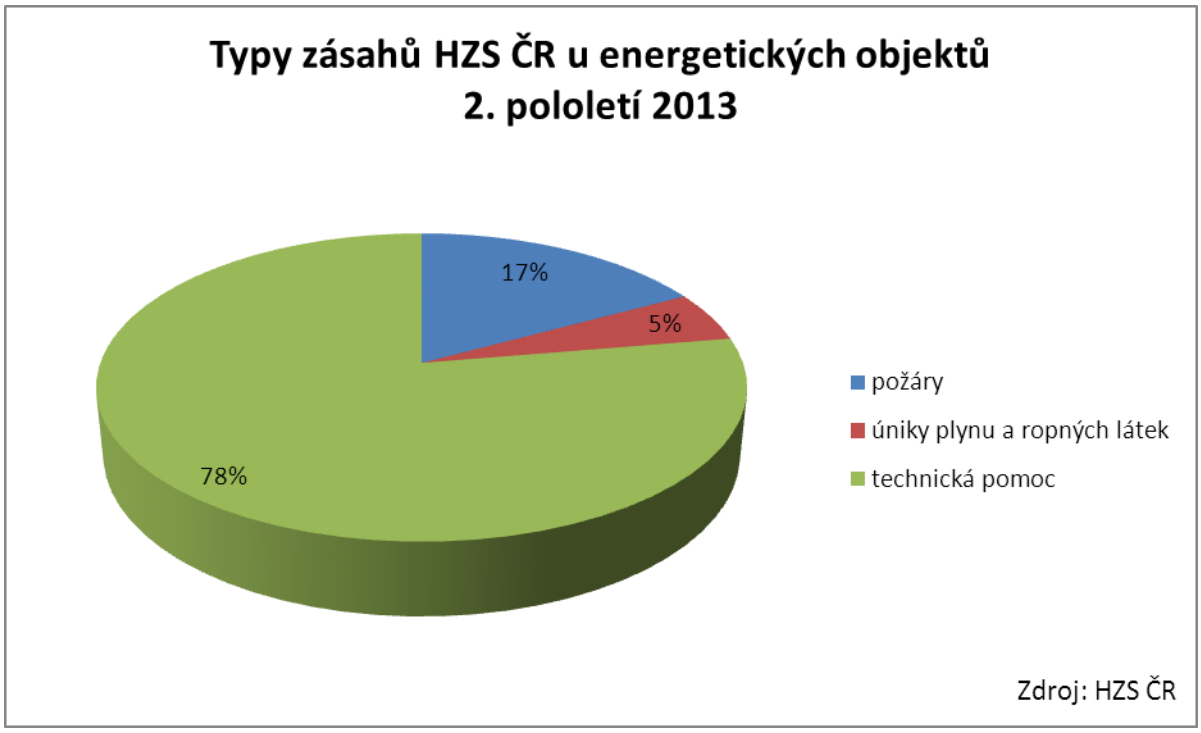
	2012	tj.%	2013	tj.%
Celkem osob	113 026	100,0	117 682	100,0
recidivisté	**56 489**	**50,0**	**61 934**	**52,6**
nezletilí do 15 let	1 371	1,2	1 251	1,1
mladiství 15 až 18 let	3 486	3,1	2 939	2,5
ženy	15 479	13,7	16 738	14,2
cizinci	7 513	6,6	7 470	6,3

Podíl recidivistů na celkovém počtu stíhaných a vyšetřovaných osob dlouhodobě stoupá. **V Moravskoslezském kraji v roce 2013 přesáhl hranici 60 %!** V roce 2013 recidivisté spáchali 77 vražd a 1 086 loupeží.

ENERGETICKÁ BEZPEČNOST

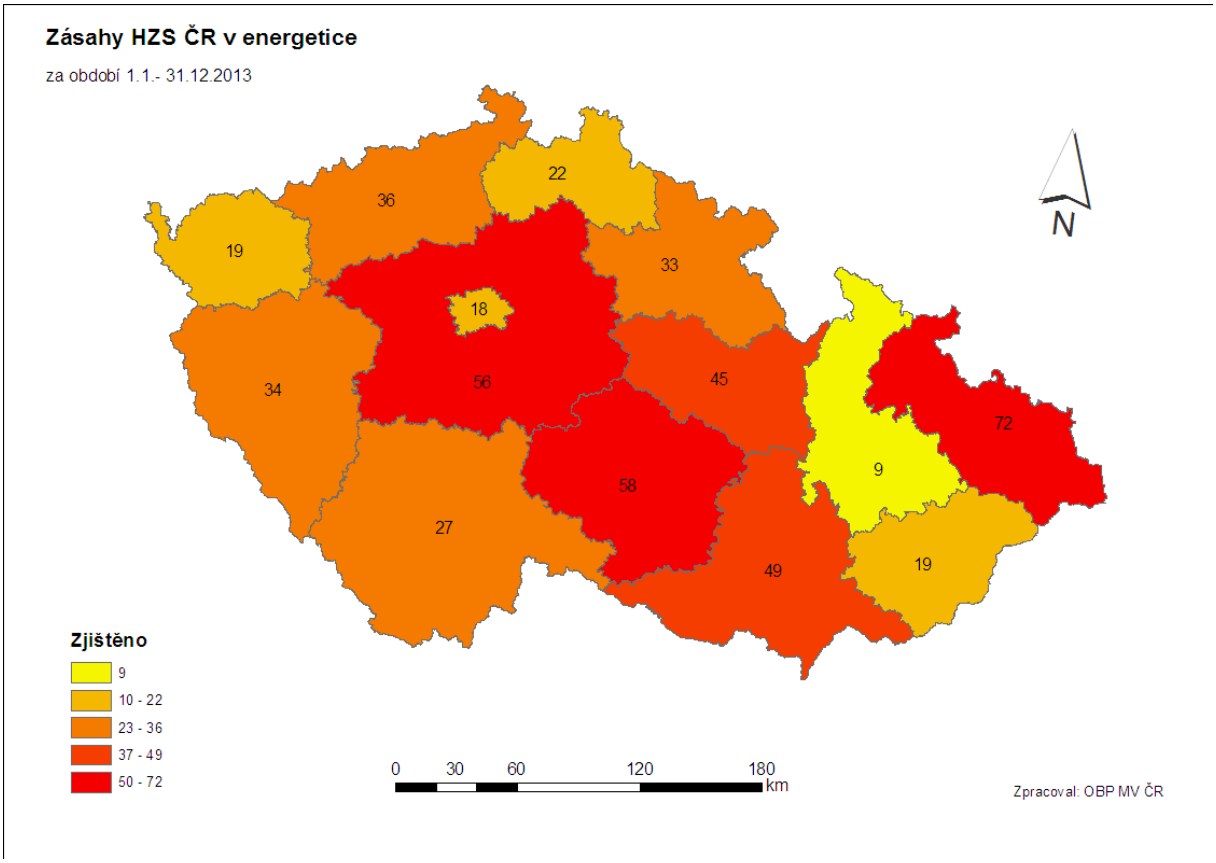
Hasičské statistiky a jejich interpretace

Ve sledovaném období (2. pololetí roku 2013) zasahovaly jednotky Hasičského záchranného sboru **celkem 497x u objektů souvisejících s energetikou**. O požáry se přitom jednalo jen v 85 případech. Dalších 13 výjezdů se uskutečnilo kvůli úniku plynu, 13 kvůli úniku ropných produktů. **Zbylých 386 výjezdů spadá do rozsáhlé kategorie „technická pomoc“** – sem patří například pády stromů na elektrické vedení, či jiné formy jejich poškození, měření koncentrace plynu, ale také například záchrana osob ze sloupů elektrického vedení. Patří sem také pokusy o sebevraždu na sloupech vysokého napětí, v některých případech bohužel úspěšné (např. v září se v pražském Střížkově na vysokonapěťovém stožáru oběsil muž; hasiči pak museli vylézt pro jeho bezvládné tělo).



Takzvaný **II. stupeň poplachu** (zapojení velkého množství hasičských jednotek) bylo však nutné vyhlásit **jen v jediném případě**, kdy došlo v prosinci k výbuchu plynu na plzeňském sídlišti Lochotín, při kterém bylo zraněno 7 osob (více o této nehodě se dozvíte v přehledu vybraných událostí na konci kapitoly). Velký požár rozvodny v pražském Chodově, který si rovněž vyžádal vyhlášení II. stupně poplachu, se odehrál již na konci 1. pololetí (více se o něm proto dočtete v předchozí Situační zprávě).

Pokud se podíváme na rozložení zásahů do jednotlivých krajů, pak stejně jako v předchozích obdobích **s velkým náskokem vede Moravskoslezský kraj**. To může být dáno množstvím energetických závodů a objektů těžby nerostných surovin v této oblasti. Vzhledem ke své poměrně nízké lidnatosti má nepoměrně velký počet zásahů také Vysočina. To může souviset s poměrně rozsáhlým poškozením energetické sítě, kterou v tomto kraji způsobil první nástup zimních mrazů.



Za první tři čtvrtiny roku 2013 (údaje za celý rok budou v průběhu příštího měsíce k dispozici na www.hzscr.cz) **byla v celkem 1 169 případech u zásahu vyžadována spolupráce pohotovostní služby elektrických rozvodných podniků a v 566 případech plynárenská pohotovostní služba**. Pokud zahrneme do statistiky všechny požáry, které měly souvislost s výrobou a rozvodem elektřiny a plynu, pak do 30. září 2013 došlo k celkem 151 takovým požárům, s celkovou škodou přes 277 milionů Kč. Zahynul při nich jeden člověk a dalších 49 bylo zraněno. Za stejné období došlo k celkem 11 požárům v odvětví těžby nerostných surovin, s celkovou škodou necelých 5,5 milionů korun.

Největší požáry související s energetikou za rok 2013

10. 6. – **Trafostanice firmy TŽ a.s.**, Třinec, okr. Frýdek – Místek.
Příčina: technická závada – elektrický zkrat na odpojovači fáze.
Škoda: 22 000 000 Kč.

18. 6. – **Trafostanice firmy ČEPS a.s.**, Praha – Šeberov.
Příčina: technická závada.
Škoda: 100 000 000 Kč.

31. 7. – **Velkokapacitní seník s fotovoltaickými panely firmy AGRA Řisuty spol. s.r.o.**, Malíkovice – Čanovice, okr. Kladno.
Příčina: nedbalost při svařování hydroizolační lepenky.
Škoda: 20 000 000 Kč; zraněni: 2 hasiči.

7. 11. – **bioplynová stanice**,
Kouty, okr. Třebíč, příčina – v šetření,
škoda – 2 500 000 Kč, požár likvidovaly 4 jednotky PO.

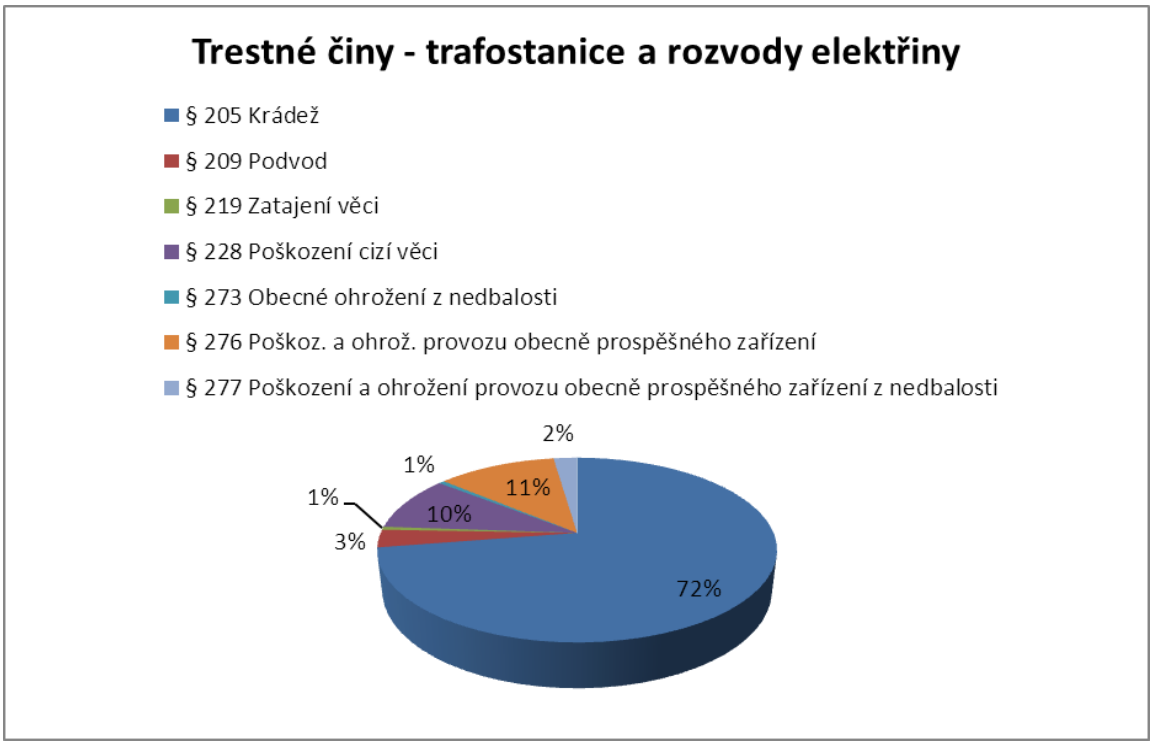
Policejní statistiky a jejich interpretace

Také letos evidovala policie větší množství trestných činů, které se dotýkaly energetické infrastruktury. Stejně jako v minulých letech dominovaly trestné činy krádeže a různé formy podvodů. Nejprve se zaměříme na kriminalitu související s elektrickou distribuční soustavou. Ty přehledně shrnuje následující tabulka:

trestné činy, kde byly objektem napadení trafostanice a rozvody elektrického proudu za období leden až prosinec 2013

registrované skutky	1 087
počet skutků, u nichž byl zjištěn pachatel	215
škoda	123 870 400 Kč

Jaká byla struktura těchto trestných činů, vidíte na následujícím grafu:



Z grafu jasně vyplývá, že v této oblasti **jednoznačně dominaje trestný čin krádeže**. Pokud se podíváme na geografické rozložení v rámci ČR, pak **nejvíce trpí rozvodná síť v důsledku krádeží v Ústeckém kraji** (celých 180 případů), v kraji Moravskoslezském (168 případů) a Středočeském (137 případů). V Praze, Pardubickém a Jihomoravském kraji se počet případů pohyboval mezi 50-60, v ostatních krajích byl výrazně nižší. Jeden jediný trestný čin krádeže v souvislosti s energetickou rozvodnou sítí pak za celý rok zaznamenal kraj Vysočina.

V této souvislosti je nutné zmínit, že **spolupráce Policie ČR a dispečinků energetických společností se stále zlepšuje**, takže se čím dál častěji daří zachytit pachatele přímo při činu. Jeden takový úspěšný zásah proběhl nad ránem 2. srpna v Miletíně na Kolínsku, kde na základě informace dispečera firmy ČEZ zadrželi policisté přímo na místě muže, který se pokoušel ukrást z transformátoru chladící olej.

Jak upozorňují zaměstnanci ČEZu, panuje bohužel velký nepoměr mezi užitkem, který má pachatel z krádeže např. pár litrů špatně upotřebitelného oleje, a škodou, kterou tímto činem způsobí. Ta se **může vyšplhat často až na 400 tisíc Kč** – poškozený transformátor je třeba vyměnit (starý zlikvidovat) a čištění okolní zeminy potřísněné olejem vychází také na pár desítek tisíc. Vzhledem k výši možného trestu za škodu takového rozsahu jde od pachatele o skutečně hloupý risk, a to nemluvíme o nemalém riziku zasažení elektrickým proudem. V tomto konkrétním případě měl přitom ukradený olej hodnotu sotva pár set korun.

V loňské Situační zprávě jsme informovali o poněkud extrémním případě zlodějů kovů, kteří rozebírali stožáry vysokého napětí tak dlouho, až dva z nich při bouřce spadly a způsobily rozsáhlé výpadky v dodávkách elektřiny. Policii se je podařilo zadržet, jejich případ projednával v listopadu 2013 okresní soud v Novém Jičíně. Před soudem nakonec stanula čtveřice mužů. Přiznal se jediný z nich, ostatní tři vinu popírali.

Údajného šéfa celé zlodějské party, patnáctkrát trestaného recidivistu, **poslal soud do vězení na tři roky**. Ostatní obžalovaní dostali podmíněné tresty, nejnižší ten z nich, který se k činu přiznal. Rozsudek ovšem není pravomocný, protože dva obžalovaní se přímo v soudní síni odvolali a případ tak poputuje ke Krajskému soudu v Ostravě. Společnost ČEZ bude muset náhradu škody, která dosahuje několika milionů korun, uplatnit u civilně-správního soudu.

trestné činy, kde byly objektem napadení
energetické závody
za období leden až prosinec 2013

registrované skutky	750
počet skutků, u nichž byl zjištěn pachatel	185
škoda	102 436 900 Kč

Jak vyplývá z výše uvedené tabulky, **energetické závody se staly terčem celkem 750 trestných činů, škoda pak přesáhla 100 milionů korun**. Nejčastějšími činy byly krádeže, podvody a poškození cizí věci.

Příkladem podvodů mohou být například **falešné účty za elektřinu**, které v listopadu zaznamenala společnost E.ON. Řadě jejích zákazníků přišel do schránky email s následujícím (či obdobným) zněním: „*Vážený zákazníku do dnešního dne tj. 7. 11. 2013 jsme neobdrželi doplatek za elektřinu. Váš nedoplatek k dnešnímu dni činí 219 Kč. Prosíme o okamžité uhrazení, aby nedošlo k navýšení částky z prodlení. Váš E.ON.*“. Následovalo několik bankovních účtů, kam mají zákazníci peníze posílat. Není třeba dodávat, že společnost E.ON nemá s uvedenými výzvami nic společného, v otázkách nedoplatků ani zákazníky touto formou neoslovuje.

Uvedený phishingový útok patří mezi ty zdařilejší a hůře odhalitelné – je psán dobrou češtinou bez zjevných gramatických chyb a byl odeslán z adresy eon.pohledavky@gmail.com (takovou adresu si ovšem může zdarma zařídit kdokoliv). **Často také falešné maily obsahují logo firmy** (opět snadno zkopírovatelné z internetu). Přesný počet lidí, kteří na falešnou výzvu zareagovali a peníze zaslali, není v tuto chvíli znám. Příprava takového trestného činu je velmi snadná a zabránit podobným útokům i do budoucna se dá zřejmě jen kvalitní osvětou.

V průběhu roku také došlo k **jednomu případu krádeže z tranzitního ropovodu** (Středočeský kraj, škoda 45 000 Kč) a ke **dvěma krádežím u tranzitního plynovodu** (Středočeský a Ústecký kraj, škoda 83 500 Kč). Pokud započítáme všechny produktovody (nejen ty tranzitní) můžeme zmínit jeden z posledních případů, který se stal těsně před koncem loňského roku. 29. prosince zloději navrtali potrubí společnosti Čepro, ze kterého se pokoušeli ukrást naftu. Kolik si jí skutečně odnesli, není zatím jisté, co ovšem jisté je, že způsobili ekologickou havárii. Hasiči museli nornými stěnami zabezpečit okolní vodoteče. Škoda z marginální krádeže se tak opět vyšplhá do výše mnoha desítek tisíc korun.

Hlavní události a trendy v evropské energetice ve II. pololetí roku 2013

Ve sledovaném období druhé poloviny roku 2013 byla energetika a energetická bezpečnost jedním z dominantních témat evropské politiky. **Předsednictví v Radě EU totiž převzala Litva, která si právě tuto oblast určila za svou prioritu**. Pro tuto pobaltskou zemi je to ostatně logická volba, neboť právě její region silně závisí na dodávkách strategických surovin z Ruska, a jeho zájmem je tak větší harmonizace společného postoje EU vůči vnějším hráčům a prosazování jednotného energetického trhu. Následující oddíl se zaměří na nejdůležitější otázky související s energetikou, které se v uplynulém pololetí projednávaly na národní i nadnárodní úrovni.

Jednotný energetický trh

Přirozenou snahou litevského předsednictví bylo další směřování k jednotnému evropskému energetickému trhu. Ten by **měl být dokončen do roku 2014**. Díky jeho fungování má dojít k posílení evropské spolupráce na poli energetiky a snížení závislosti na Rusku. Samotné Litvě vyprší v roce 2015 smlouva na dodávky ruského plynu, a bude se jí proto hodit co nejsilnější vyjednávací pozice pro sjednání nových podmínek. Z Ruska zatím Litva dováží veškerý svůj zemní plyn. Od roku 2015 by však měl v Klajpedě fungovat terminál pro dovoz zkapalněného zemního plynu, který umožní jistou diverzifikaci.

Podle Litevců musí EU posilovat spolupráci členských států ve vztazích k dodavatelům energetických zdrojů. Předsednická země se také s Komisí podílela na přezkoumání a aktualizaci vodítek pro vnější dimenzi energetické politiky, která byla stanovena v roce 2011.

Cílem nového síťového kodexu z dílny Evropské komise je lépe rozdělit přeshraniční kapacity přenosu energie a usnadnit tím vytvoření ničím nerušeného celoevropského trhu s elektřinou. Takové obchodování by podle EU mělo být rychlejší a ušetřit miliardy eur ročně. Nynější plán Bruselu by měl **srovnat podmínky prodeje energie za hranice jednotlivých zemí**. Přenosová kapacita pro přeshraniční dodávky elektřiny je totiž omezená, což vytvoření jednotného trhu značně ztěžuje. Na základě speciálně vytvořeného algoritmu se mají nově na burze obchodovat nabídky jednotlivých obchodníků v propojených trzích do výše dostupné kapacity pro přeshraniční přenos.

Obchodníkům by se tím snížila rizika a nejistoty. Ti totiž často nevěděli, zda se jim podaří výhodně nakoupit energii a zároveň budou mít i kapacitu k jejímu přenosu. Na jednotném trhu však probíhá obojí automaticky. Další výhodou by mělo být i **optimální zapojení zdrojů do soustavy**. Čím větší je oblast propojená pomocí přeshraničních kapacit, tím větší existuje konkurence a také šance uplatnit případné přebytky elektřiny.

Na začátku uplynulého roku bruselští úředníci odhadovali, že by k odstranění energetických hranic mohlo dojít do konce roku 2014. Teď se mluví spíše o roce 2015. Propojení totiž musí předcházet sladění osmadvaceti různých systémů obchodování s energiemi, časů obchodování i konstrukce ceny. Například počítačové systémy jednotlivých burz nejsou v tuto chvíli vzájemně kompatibilní. **Vytvoření jednotného trhu proto znamená investice v řádu milionů eur**. O náklady na vznik a provoz systému by se přitom měli dělit provozovatelé jednotlivých národních burz a provozovatelé přenosových soustav. EU na něj neplánuje poskytovat žádné dotace. Pro Českou republiku je v tuto chvíli klíčová zejména Evropská energetická burza v německém Lipsku, kde obchoduje např. společnost ČEZ.

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

Plnění cílů 20-20-20

Horkým tématem uplynulého pololetí bylo plnění klimaticko-energetických cílů EU do roku 2020 a debata o stanovení nových do roku 2030. Ukazuje se, že Evropská unie bude podle všeho schopná **naplnit pouze dva ze tří cílů**, které si do roku 2020 stanovila:

1. pokles emisí skleníkových plynů o 20 % oproti roku 1990;
2. 20% podíl obnovitelných zdrojů v energetickém mixu;
3. zvýšení energetické účinnosti o 20%.

Podle zprávy Evropské agentury pro životní prostředí činí největší potíže právě poslední, třetí cíl, k jehož splnění se v současné době blíží pouze čtyři členské státy. Ten byl také jako jediný nezávazný. Naopak splnění prvních dvou cílů se zdá poměrně reálné, pokles emisí skleníkových plynů by mohl být dokonce o několik procentních bodů vyšší, než smluvených 20%. Lépe tak dopadnou i závazky vůči Kjótskému protokolu, a to odhadem o 5,5%.

Celkově zřejmě nebude v Evropě žádná země, která by splnila všechny tři cíle. Šest zemí bude mít problém s dodržením emisních závazků (Belgie, Irsko, Finsko, Lucembursko, Rakousko a Španělsko), dalších šest se zatím potýká s plněním průběžných cílů v oblasti obnovitelných zdrojů energie (Belgie, Francie, Lotyšsko, Malta, Nizozemsko a Velká Británie).

Klimaticko-energetické závazky pro rok 2030

V letošním roce unie zintenzivnila jednání o nastavení nových cílů do roku 2030. Diskusi zahájila Evropská komise již na jaře vydáním tzv. **zelené knihy**, která představila obecný rámec pro klima a energetiku pro příští dvě desetiletí. Dlouhodobým cílem do roku 2050 pak má být snížení emisí oproti roku 1990 až o 90%. V důsledku hospodářské krize a rozpočtových problémů řady evropských zemí je ale shánění prostředků na dlouhodobé investice v energetice čím dál náročnější. Přesto Komise **navrhla do roku 2030 snížení emisí alespoň o 40%**, přičemž tento závazek je podle ní reálný i bez nadměrného navýšení nákladů na výrobu energie.

Přes tlak různých ekologických organizací, které prosazují ještě ambicióznější závazky, se nicméně zdá, že snižování emisí zůstane jediným cílem, který Evropa označí jako závazný. Ostatní dva, týkající se nových standardů pro energetickou účinnost a podíl obnovitelných zdrojů, **budou mít zřejmě pouze doporučující charakter**. Tuto variantu dle všeho podporuje většina evropských zemí, podle ředitele odboru energetiky a ochrany klimatu Pavla Zámyslického je mezi nimi i Česká republika. Na samém začátku roku 2014 sice výbory Evropského parlamentu pro průmysl, výzkum a energetiku (ITRE) a pro životní prostředí, veřejné zdraví a bezpečnost potravin (ENVI) podpořily navázání na současný trend tří závazných cílů, hlavní slovo bude mít ale Evropská komise, která se zřejmě pod tlakem většiny států přikloní k variantě jednoho závazného cíle a dvou doporučených.

Největší debata se opět vede nad otázkou **nastavení závazků energetické účinnosti**, jejichž plnění je ze současných cílů nejproblematičtější. Na schválení tohoto cíle velmi tlačí také některé složky stavebního průmyslu, pro které by znamenal možnost značných zakázek na zateplování

staveb. Že by cíle měly být tři, a to skutečně ambiciózní, je přesvědčena také nevládní organizace Greenpeace. Ta do roku 2030 prosazuje snížení emisí CO2 nejméně o 55 % ve srovnání s rokem 1990, zvýšení podílu obnovitelných zdrojů na 45 % a zvýšení energetické účinnosti a úspor v rozsahu 40 % spotřeby primárních zdrojů energie v roce 2005.

Regulace evropského trhu emisních povolenek

Důležitým tématem na evropské úrovni bylo ve druhé části roku 2013 **jednání o definitivní podobě backloadingu**, tedy dočasného stažení 900 milionů emisních povolenek. Evropská komise přišla s dalším nápadem, který by měl systému emisního obchodování pomoci dlouhodobě. Počet povolenek na trhu by mělo být podle nového plánu možné regulovat s větší flexibilitou.

Státní program na podporu úspor energie 2014

Vláda schválila 20. listopadu 2013 program na podporu úspor energie a využití obnovitelných a druhotných zdrojů energie 2014. Program je zřízen na základě ustanovení § 5 tohoto zákona a je také jedním z nástrojů pro zajištění mezinárodních závazků, zejména snížení podílu spotřeby energie na HDP o 1 % ročně (podle směrnice č. 2006/32/ES), zvýšení podílu elektřiny z obnovitelných zdrojů na 20 % a snížení spotřeby energie o 20 % v roce 2020 (podle Strategie Evropa 2020). V roce 2013 byl navíc přijat národní cíl úspory 47,84 PJ na konečné spotřebě energie do roku 2020. *Prioritou programu je osvěta a vzdělávání laické i odborné veřejnosti, pomoc statutárním městům a krajům se zaváděním energetického managementu a podpora malých investičních akcí s přímými úsporami energie zejména pro města a obce, ale též pro menší podnikatelské projekty,"* uvedl ministr průmyslu a obchodu Jiří Cienciala. V porovnání s operačními programy nemá program EFEKT významný rozpočet, pro rok 2014 bylo vyhrazeno 30 mil. Kč, ale přesto hraje velkou roli zejména v oblastech, které nelze financovat ze strukturálních fondů EU.

Trh s emisními povolenkami by mohla Evropská unie usměrňovat podobně, jako centrální banky regulují měnové kurzy. Nový plán by měla představit ještě během podzimu, poté bude zahájena veřejná konzultace. Od změny si exekutiva slibuje, že posílí skomírající systém emisního obchodování (EU ETS). Ceny emisních povolenek jsou v současné době příliš nízké na to, aby podniky motivovaly k investicím do úspornějších technologií. Na trhu je totiž přebytek povolenek, který vznikl zejména v důsledku ekonomické krize.

Komise proto v roce 2012 navrhla, aby se ze systému aukcí dočasně stáhlo určité množství povolenek – konkrétně má jít o 900 milionů. Evropský parlament tento návrh nakonec podpořil a čekalo se na rozhodnutí členských států. Nový plán by však přinesl další změnu. Jak již bylo naznačeno, **počet povolenek na trhu by mělo být možné regulovat mnohem flexibilněji než doposud**. Jejich množství by se mělo upravovat pravidelně, pravděpodobně s odstupem tří měsíců. V současném systému je přitom počet stanoven na období čtyř let a zůstává neměnný bez ohledu na makroekonomický vývoj. Panuje totiž všeobecné přesvědčení, že systém emisního obchodování v každém případě dlouhodobou reformu potřebuje. Dočasné stažení 900 milionů povolenek je tudíž považováno pouze za dočasné řešení.

Summit V4 v Budapešti

Energetika a zejména energetická bezpečnost patřily mezi **hlavní témata říjnového summitu premiérů visegrádské čtyřky**. Ministerští předsedové Maďarska, Polska, Slovenska a České republiky se sešli v Budapešti. Maďarsko od července 2013 do června 2014 visegrádské skupině předsedá.

Jednou ze tří hlavních priorit maďarského předsednictví je právě energetická bezpečnost. Pod vedením premiéra Viktora Orbána se chce Maďarsko zaměřit hlavně na rozvoj vnitřního trhu s

energií, který by měl být dokončen již do roku 2014. Dalším silným tématem je diverzifikace zdrojů, ať už jde o projekty tzv. Jižního koridoru nebo například rozvoj importních terminálů pro zkapalněný zemní plyn (LNG).

Maďarské předsednictví se chce zaměřit také na pokračující **integraci trhu s plynem v regionu střední Evropy**. Visegrádská čtyřka k tomu letos v červnu přijala cestovní mapu. Premiéři probírali i otázky spojené s využíváním nekonvenčních ložisek zemního plynu, tedy zejména zásob břidlicového plynu. Shodli se, že **každá z členských zemí Evropské unie by měla mít právo rozhodovat sama o složení svého energetického mixu**, a tedy i o případném využití těchto nekonvenčních ložisek.

„Těžba břidlicového plynu je pro naše země důležitým aspektem, pokud jde o diverzifikaci dodávek zemního plynu," řekl na tiskové konferenci po jednání polský premiér Donald Tusk. „Všichni jsme vyjádřili zásadní názory našich zemí, pokud jde o oblast energetiky. Dohodli jsme se na vzájemné podpoře jak v oblasti jaderné energetiky, tak v oblasti suverenity členských zemí v rozhodování o tom, jaké zdroje primární energie budou využívat – včetně možností, které některým z nás dává potenciál břidlicového plynu," shrnul jednání český premiér v demisi Jiří Rusnok.

Pokud jde o jadernou energetiku, premiéři Visegrádu jednali mimo jiné o **společném postoji k návrhu na revizi směrnice o jaderné bezpečnosti**, který měla Evropská komise zveřejnit rovněž v říjnu. Revize by měla reagovat na katastrofu v japonské Fukušimě z roku 2011, která se dotkla i tamní jaderné elektrárny. Novela má posílit harmonizaci bezpečnostního rámce a hodnocení jaderné bezpečnosti a rozšířit vzájemné posuzování bezpečnosti jaderných zařízení provozovaných jednotlivými státy.

Země V4 se shodují na tom, že téma jaderné energetiky by se nemělo politizovat. „Slovensko respektuje, že v Evropské unii některé státy jadernou energii využívat nechtějí, ale očekáváme také, že budou respektovány i ty země, které jádro využívají. Nedovedu si představit, že by Evropská komise převzala v této oblasti významnější pravomoci, které patří národním státům," řekl k tématu slovenský ministerský předseda Robert Fico.

Podobný názor na tiskové konferenci vyjádřil i maďarský premiér Viktor Orbán. „Očekáváme, že Evropská unie bude pomáhat, a nikoli bránit zvyšování jaderných kapacit ve střední Evropě," řekl Orbán. Jak dodal, měla by se rovněž přezkoumat problematika státní podpory pro investice do jaderné energetiky. „Myslíme si, že jaderná energetika je zde diskriminována," řekl Orbán. Zatímco Německo či Rakousko jsou proti jaderné energii, Británie či právě státy V4 s ní problém nemají. Velká Británie dokonce ve sledovaném období Situační zprávy oznámila záměr výstavby zcela nové jaderné elektrárny.

Společným problémem zemí V4 jsou také **neplánované toky elektřiny ze severu Německa**, kde bylo v posledních letech instalováno velké množství větrných elektráren, na jih Německa a do Rakouska, kde je velká spotřeba. Kvůli nedostatečné kapacitě vnitroněmeckých sítí totiž vyprodukovaná elektřina přetěžuje síť v České republice a Polsku. I díky visegrádské spolupráci se téma podařilo prosadit do závěrů květnové Evropské rady mezi činnosti, které je potřeba v souvislosti s dokončením trhu s elektřinou řešit.

Cvičení RESTART 2013

Dne 4. září 2013 proběhlo dosud nejrozsáhlejší elektroenergetické cvičení v České republice. V jeho rámci se prověřovala spolupráce při vyhlášení stavu nouze v české přenosové soustavě a výpadku proudu na části území ČR. Při řešení této situace a jejích následků se procvičila vzájemná komunikace a koordinace všech dotčených subjektů. Do cvičení byly zapojeny stovky zaměstnanců z Ministerstva průmyslu a obchodu, ČEPS, ČEZ Distribuce, složek integrovaného záchranného systému, krizových štábů, municipalit i veřejnoprávních médií.

Cvičení RESTART simulovalo přetížení a rozpad jednotné evropské sítě, který způsobí sérii výpadků elektřiny po celé Evropě. Současně v České republice větrná smršť poškozuje stožár s vedením elektrického proudu, které se automaticky vypíná. Rozvodny Týnec, Krasíkov a Neznášov ve východních Čechách jsou tak závislé pouze na jednom jediném vedení, v jehož blízkosti navíc vzniká požár, takže se nakonec ocitají zcela bez proudu. Nastává lokální blackout, který se dotkne přibližně 700 000 lidí v Pardubickém a Královéhradeckém kraji.

Bez elektřiny jsou nejen domácnosti, ale i obchody, nemocnice a další veřejné instituce, alarmy jsou vypnuté. Běžné telefony nefungují nebo se brzy vybijí. Kolabuje doprava, vlaky nejezdí nebo jim hrozí riziko srážky, autům dochází benzín, semafory i veřejné značení nesvítí. Zasedá krizový štáb společnosti ČEPS, který rozhoduje o vyhlášení stavu nouze pro celou Českou republiku.

ČEZ Distribuce spouští intenzivní komunikaci se zainteresovanými subjekty, do terénu vyjíždějí stovky techniků, aby opravovali poškozená zařízení. Přístup jim ale ztěžuje rozmáčený terén a popadané stromy. To je práce pro hasiče se speciální technikou. Hasičský záchranný sbor v rámci RESTARTu nacvičoval také záchranu zraněné osoby ze stožáru vysokého napětí. Na řadu proto přišli i záchranáři, důležitou roli měli také policisté. Ti musejí při blackoutu mj. hlídat místa s velkou koncentrací osob, řídit dopravu a zajistit, aby nedošlo k porušování zákonnosti (například rabování). O celé situaci je nutné informovat také místní úřady a média. Dalším účastníkem cvičení byla i Správa železniční a dopravní cesty, která musela reagovat na výpadky napětí v trakční soustavě a zastavení provozu na elektrifikovaných tratích. Bylo tak nutné zajistit odklony osobních i nákladních vlaků a zajistit náhradní autobusovou dopravu. Staniční a traťová zabezpečovací zařízení musela být napájena ze záložních baterií či jiných náhradních zdrojů elektrické energie.

Během cvičení byl využit i speciální stavebnicový systém, schopný v krátkém čase přemostit poškozenou část přenosové trasy. Náhradní přenosová trasa byla v rámci cvičení postavena dle předem stanoveného harmonogramu a potvrdila se tak její užitečnost pro podobné krizové situace.

Cvičení začalo v šest hodin ráno, díky součinnosti všech zmíněných složek proto mohl být již v 17:45 ukončen stav nouze. ČEZ Distribuce nicméně ještě pokračoval v odstraňování jednotlivých poruch na vysokém a nízkém napětí. Napájení všech odběratelů z distribuční soustavy bylo obnoveno před polednem následujícího dne a tím došlo k ukončení celého cvičení RESTART.

Vybrané události ve sledovaném období

Červenec

Nový informační systém pro dispečery ČEPS

Nový Situační Geoprostorový Systém (SGS) zajišťuje vizuální analýzu dat z mnoha zdrojů v prostoru a čase. Umožňuje dispečerům spolehlivěji řídit přenosovou soustavu díky komplexnějším informacím o meteorologické situaci (teplota, blesky, směr a síla větru, námraza, sluneční svit atd.) a aktuálním stavu přenosové soustavy. Získaná data jsou znázorňována blízko reálnému času - historické informace i predikce jsou zobrazovány v časovém horizontu 48 hodin. Systém zároveň umožňuje přesně lokalizovat případné poruchy. Tento nový nástroj zvyšuje efektivitu dispečerského řízení, omezuje rizika a posiluje spolehlivost přenosové soustavy.

Středoevropské země podepsali memorandum, směřující k další integraci trhu s elektřinou

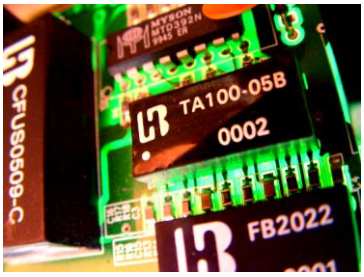
Zástupci regulačních úřadů (ERÚ, ÚRSO, HEA, URE a ANRE), provozovatelů přenosových soustav (ČEPS, SEPS, MAVIR, PSE a Transelectrica) a operátorů trhu (OTE, OKTE, HUPX, TGE a OPCOM) České republiky, Slovenska, Maďarska, Polska a Rumunska dne 11. července 2013 podepsali Memorandum o porozumění o spolupráci na přistoupení Rumunska a Polska k propojenému česko-slovensko-maďarskému dennímu trhu s elektřinou.
Česká republika, Slovensko a Maďarsko provozují úspěšně společný denní trh s elektřinou (tzv. CZ-SK-HU Market Coupling) od 11. září 2012. Rumunsko a Polsko se rozhodly připojit se k tomuto třístrannému projektu s cílem podílet se na benefitech integrace a přispět tak k rozvoji jednotného evropského trhu s elektřinou. Propojení národních trhů s elektřinou na základě cílového modelu – tzv. Single Price Market Coupling pro denní obchody s elektřinou a implicitní alokace přeshraničních kapacit – by mělo zajistit harmonizovaný přístup k organizaci trhu, efektivnější využití přeshraničních přenosových kapacit, zvýšení konkurence na trhu, stabilizaci a konvergenci velkoobchodní ceny elektřiny a nárůst likvidity trhu.
Pentalaterální projekt nese anglické označení 5Market Market Coupling (zkráceně 5M MC) a bude rozvíjen v souladu s evropskými cíli a budoucí legislativou EU při respektování názorů a požadavků dotčených účastníků trhu.

Ruská společnost Rosněft' bude dodávat ropu do ČR

Ruská státní ropná společnost Rosněft' podepsala tříletou dohodu s největší polskou rafinerskou skupinou PKN Orlen o dodávkách ropy do České republiky přes ropovod Družba. Do konce června 2016 by měla firma dodat do Česka asi 8 milionů tun ropy za 7 miliard dolarů. Dodávky pokryjí 60 až 100 procent poptávky Unipetrolu. S ropovodem Družba byly přitom v minulosti problémy kvůli omezení dodávek. Podle analytiků probíhá v současnosti konkurenční boj mezi ruskými těžařskými firmami, vstupem Rosněfťu se tak omezí dominantní postavení firem Lukoil a Gazprom.
Prodloužena byla i smlouva u přepravy ropy ze západu, přes ropovod TAL z italského Terstu a jeho prodloužení IKL. Dodatek ke smlouvě platí až do roku 2015. Díky IKL má ČR pojistku proti případnému přerušení dodávek přes Ukrajinu.

Srpen

Senzory používané v energetice jsou náchylné ke kybernetickému útoku
Výzkumníci Lucas Apa a Carlos Mario Penagos z IOActive studovali senzory vyráběné třemi hlavními výrobci bezdrátových zařízení automatizačních systémů. Tato zařízení jsou široce používána pro distribuci energie, vody, zemního plynu, jaderné energie, ropy a u rafinérských ropných společností. Jednalo se o senzory komunikující s řídícím střediskem rádiovými vysílači v pásmu 900 MHz nebo 2,4 GHz, a hlásící provozní a kritické údaje o chodu distribučních systémů ze vzdálených míst. Výsledky výzkumu byly prezentovány na konferenci o kybernetické bezpečnosti Black Hat. Výzkumníci našli řadu softwarových zranitelností. Mnohá z čidel obsahovala nedostatky typu slabé kryptografické klíče používané k potvrzování pravosti komunikace, softwarové zranitelnosti a konfigurační chyby. Výzkum například objevil několik skupin senzorů dodaných s identickými kryptografickými klíči, možnost odpojit všechny senzory při porušení paměti zařízení, nebo vypnout celé zařízení a možnost upravit hodnoty, které senzory hlásí. A to vše ze vzdálenosti až 40 mil (cca 64 km).



Vzhledem k tomu, že útok není veden přes internet, neexistuje žádný snadný způsob, jak takovou škodlivou činnost či pachatele vystopovat. Jednoduchá nebude ani náprava současného neuspokojivého stavu. Náprava bude vyžadovat aktualizaci firmwaru a změny konfigurací. Protože senzorové sítě zahrnují velké množství senzorových uzlů s omezenými hardwarovými možnostmi, tak distribuce nových a zrušení starých klíčů, případně aktualizace firmware, nebudou snadné ani rychlé.
Vzhledem k závažnosti zjištěných chyb nemohou být z důvodu bezpečnosti blíže veřejně specifikována dotčená zařízení ani jmenovány společnosti, jejichž zařízení jsou těmito zranitelnostmi zasažena. Proto také nebudou informovány tyto společnosti, ale přímo národní organizace U.S. Computer Emergency Readiness Team (US-CERT's), která stanoví koordinovaný a bezpečný postup nápravy. Zprávu přineslo Národní centrum kybernetické bezpečnosti (NCKB).

Policie zadržela zloděje transformátoru přímo při činu
V Miletíně na Kolínsku se díky dobré spolupráci Policie ČR a dispečerů ČEZ podařilo zadržet pachatele, který se pokoušel z transformátoru ukrást chladící olej. Více informací o tomto případu naleznete v první části této kapitoly, věnované policejním statistikám.

Závada trafostanice v pražském Chodově zastavila provoz metra i tramvají
20. srpna odpoledne vypadl na několik minut proud v Praze 4 a části Prahy 10 a Prahy 2. Příčinou byla technická závada v trafostanici na pražském Chodově. Krátkodobý výpadek omezil nejen dodávku elektřiny do zhruba stovky tisíc domácností, ale také na několik minut zcela zastavil metro a většinu pražských tramvají. K výpadku došlo v souvislosti instalací nového transformátoru. Stejná rozvodna měla přitom problémy již v červnu, kdy zde vypukl požár, po kterém zůstala bez proudu téměř polovina Prahy. Škoda tehdy dosáhla desítek milionů korun.

Září

Seminář o roli přenosové soustavy při ochraně národní kritické infrastruktury
Na Krajském vojenském velitelství Ostrava proběhl 10. 9. 2013 seminář o bezpečnostní problematice národní kritické infrastruktury, který byl věnován zejména energetické přenosové soustavě. Více informací naleznete v kapitole Krizové řízení.

Nový kompresor pro zásobník zemního plynu v Lobodicích
Unikátní zásobník zemního plynu v Lobodicích na Přerovsku spustil nový kompresor za 100 milionů korun. Provoz, který distribuuje plyn na severní i jižní Moravu a stát ho využívá k doplnění

výpadku dodávek, tak teď funguje mnohem pružněji. Nový kompresor podzemnímu zásobníku v Lobodicích sice nezajišťuje větší kapacitu, zato je nyní provoz mnohem výkonnější.
V případě potřeby ho pracovníci mohou z režimu vtlačování plynu přepnout do těžebního v řádu několika málo hodin. Jinde to trvá až několik dní. Zásobník zemního plynu v Lobodicích je zajímavý hned z několika důvodů. Je se svou kapacitou 100 milionů kubických metrů vůbec nejmenším a zároveň nejstarším podzemním zásobníkem plynu v republice, funguje už od roku 1965. Lobodice jsou však zřejmě na dlouhou dobu posledním podzemním zásobníkem, který se dočkal tak velké investice. Kvůli nejistotě, co s plynem bude dál a také kvůli malému zájmu obchodníků, se skupina RWE rozhodla další projekty, zaměřené na navýšení skladovací kapacity, pozastavit.

Velká exploze plynového zásobníku v Německu donutila k evakuaci 3000 lidí

Na západě Německa nad ránem během požáru v podniku pracujícím s plynem explodoval plynový zásobník. Výbuch zranil 17 hasičů, jednoho z nich vážně. Záchranáři následně rozhodli o evakuaci celé přilehlé vesnice Harthausen se zhruba 3000 obyvateli. Hořet začalo nad ránem v podniku, který pracuje s plynem. Během hašení se však požár dostal až k zásobníku plynu, který následně explodoval. Po výbuchu se zhroutila budova skladu. Výbuch byl slyšet i v nedalekém Ludwigshafenu a Mannheimu. Na místě zasahovalo přes 160 hasičů, kteří nechali ohrožené plynové zásobníky kontrolovaně vyhořet.

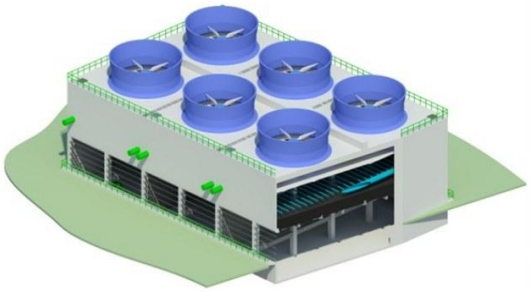
Podle studie německých Zelených má Temelín konstrukční nedostatky. Česká strana to odmítá.
Podle posudku vypracovaného na podnět německé strany Zelených představují svary mezi tlakovou nádrží a primárním bezpečnostním okruhem v Temelíně bezpečnostní riziko. Informaci přinesl deník Der Spiegel. Podle posudku je dokumentace ke svařovacím pracím neúplná, obsahuje chyby a částečně si odporuje. Pochybnosti o kvalitě svarů se objevily již v minulosti, čeští experti ale při kontrolách žádné nedostatky neodhalili. Společnost ČEZ i Státní úřad pro jadernou bezpečnost se proto žádné případné další kontroly neobávají. Německý ministr životního prostředí navíc odmítl návrh poslanců Zelených, aby si na Česku vyžádal další zkoušky. Předsedkyně SÚJB Dana Drábová vidí v novém posudku spíše formu předvolebního boje v Německu.

Hasiči si vyzkoušeli chlazení temelínského reaktoru vodou jako ve Fukušimě
Hasiči temelínské elektrárny provedli cvičení, během kterého simulovali chlazení reaktoru vodou prostřednictvím mobilního čerpadla. Tato varianta by byla nezbytná v případě selhání několika záložních systémů elektrického napájení elektrárny – k podobné situaci došlo například při havárii v japonské Fukušimě. Více informací o tomto cvičení naleznete v kapitole Krizové řízení.

Říjen

Distribuční společnosti zahájily odorizaci plynu před zimní topnou sezónou
Některé distribuční společnosti (např. Pražská plynárenská) přistoupily v říjnu po předchozích pozitivních zkušenostech opět k nárazové odorizaci zemního plynu, která má lidem usnadnit detekci jeho úniku, a zabránit tak případným nehodám a mimořádným událostem. Při tomto procesu je zemní plyn nasycen dvojnásobným množstvím látky s charakteristickým intenzivním zápachem, který umožní i běžným odběratelům zaznamenat i velmi drobné netěsnosti v rámci plynových rozvodů, které by byly jinak bez přístrojového vybavení těžko zjistitelné.
Pražská plynárenská provedla nárazovou odorizaci již v květnu 2013 a podařilo se díky ní odhalit zhruba 88 úniků v rámci bytových instalací či domovních rozvodů. Na základě této pozitivní zkušenosti byla provedena další odorizace před zimní topnou sezónou. Úspěch tohoto opatření pochopitelně závisí také na dobrém informování veřejnosti.

Nové ventilátorové věže zvýší odolnost Dukovan proti extrémním živlům



JE Dukovany dostala od Ministerstva průmyslu a obchodu stavební povolení ke stavbě nízkých, velmi odolných ventilátorových věží, učených především ke chlazení bezpečnostních systémů elektrárny. Výstavba jednoho z těchto objektů pro 1. a 2. blok elektrárny začne na jaře 2014, dokončena bude do roku 2015. Vysoké budou pouhých 17 metrů, oproti více než stometrovým chladícím věžím, které v současnosti dominují siluetě elektrárny. Původní věže přitom zůstanou zachovány pro chlazení kondenzátorů turbín. První objekt, blok šesti ventilátorových věží pro chlazení tří bezpečnostních systémů 1. a 2. bloku, bude na západní straně elektrárny v blízkosti současných chladících věží. Druhý identický objekt pro systémy 3. a 4. bloku bude stavěn o dva roky později na východním konci elektrárny.
Protože výška ventilátorových věží je jen cca 1/10 výšky současných věží nebude kolemjdoucí vidět prakticky žádnou změnu. Ta bude spočívat pouze ve zvýšení odolnosti elektrárny proti extrémním přírodním situacím, jako jsou velké zemětřesení, tornádo, nebo dlouhotrvající extrémní teploty. Potřeba vybudovat v Dukovanech odolnější chladicí věže vyplynula ze zátěžových testů prováděných po předloňské havárii japonské elektrárny Fukušima.

Slovensko a Polsko možná propojí nový plynovod s norským plynem.
Slovensko a Polsko chtějí rozšířit plynárenské trasy a posílit energetickou nezávislost na Rusku. Přepojení má být součástí plánovaného Severojižního koridoru, který bude vést od norského pobřeží po chorvatský ostrov Krk. Investory nového plynovodu mají být slovenská firma Eustream a její polský kolega Gaz-System. Informovala o tom slovenská tisková agentura SITA.

Listopad

Zloději kovů, kteří způsobili pád stožárů u soudu
Okresní soud v Novém Jičíně uzavřel případ čtveřice mužů, kteří zavinili pád dvou stožárů elektrického vedení nedaleko Příbora. Údajného šéfa party poslal soud do vězení, ostatní dostali podmíněné tresty. Rozsudek není pravomocný, protože někteří účastníci řízení se proti němu na místě odvolali. Více informací o tomto případu naleznete v části věnované policejním statistikám na začátku této kapitoly.

Praha chce udělat cvičný blackout
Pražský magistrát oznámil svůj záměr uspořádat cvičení, které by prověřilo připravenost města na rozsáhlý výpadek elektřiny. Jedním z motivů k jeho uspořádání byl i červnový požár trafostanice na Chodově, po kterém zůstala bez proudu téměř polovina Prahy. Více informací o tomto cvičení, které by se mělo konat v prvním čtvrtletí roku 2013, naleznete v kapitole Krizové řízení.

Maďarsko je odhodláno dokončit South Stream
Maďarská ministryně pro národní rozvoj, Németh Lászlóné ve svém proslovu na konferenci South Stream: *The Evolution of a Pipeline* v Budapešti potvrdila, že Maďarsko je i nadále odhodlané pro dokončení výstavby plynovodu South Stream. Zdůraznila, že Jižní proud svou pozemní evropskou trasou vytvoří chybějící spojení mezi státy a přispěje k posílení energetické bezpečnosti Střední Evropy.
Rusko samozřejmě zůstane i nadále prioritním strategickým partnerem, Maďarsko je totiž poměrově největším odběratelem plynu ve Střední Evropě. Projekt South Stream dává příležitost k diverzifikaci tras vývozu ruského plynu i snížení závislosti dodavatelů a odběratelů plynu na tranzitních zemích.
Maďarská rozvojová banka a Gazprom podepsali dohodu o spolupráci při budování plynovodu a přepravě zemního plynu přes Maďarsko v březnu 2009. Dne 31. října 2012, během návštěvy

náměstka předsedy Gazprom A. Medveděva v Budapešti bylo přijato konečné investiční rozhodnutí o výstavbě maďarské části plynovodu.

V pondělí, 18. listopadu 2013 byl South Stream prohlášen za prioritní investiční projekt. Ministryně Németh Lászlóné potvrdila, že přípravy maďarské trasy plynovodu pokračují dobře. Pál Kovács, státní tajemník odpovědný za energetiku naléhal na zapojení Evropské unie do jednání s Ruskem o energetických záležitostech. Dodal, že Střední Evropa potřebuje okamžité řešení na zvýšení bezpečnosti dodávek energie. S plánovanými rozvoji infrastruktury se v regionu může zrodit trh plynu konkurenceschopné velikosti. Zvýšení transparence může snížit nedodělky trhu plynu oproti trhu elektrické energie.

ČEZ nepřijde o bulharskou licenci

Bulharský energetický regulační úřad (DKEVR) nenašel důvod, kvůli kterému by mohl odebrat licenci tamní pobočce českého energetické společnosti ČEZ. Bulharský regulátor, který o možném odebrání licence jednal od dubna, proto řízení z ČEZ zastavil. Na počátku roku se české firmy ČEZ a Energo-Pro a rakouská EVN, které zajišťují v Bulharsku distribuci elektřiny, staly terčem masových protestů Bulharů kvůli vysokým fakturám.

Prosinec

Výbuch plynu na plzeňském sídlišti Lochotín

12. prosince došlo v ulici Elišky Krásnohorské v Plzni k výbuchu plynu, který zranil sedm dělníků, kteří vyměňovali uzávěry na potrubí. Jednoho z nich převezla záchranka v kritickém stavu na popáleninové centrum v pražských Vinohradech, u dalších čtyř se jedná o vážná zranění. K nehodě došlo při plánované rekonstrukci plynovodu, bez dodávek zůstalo asi tisíc odběratelů v bezprostředním okolí místa nehody. Výbuch poškodil i síť provozovatele internetového připojení PilsFree, díky čemuž neměli další tisíce lidí přístup na web. Na místě zasahovalo pět jednotek hasičů, kteří zde postavili i týlový kontejner, protože se jednalo o dlouhodobý zásah.

Nové vedení vysokého napětí vyřeší nedostatek elektřiny v Libereckém kraji

Po několik předchozích let byli energetici nuceni odmítat nové odběratele kvůli nevyhovujícímu systému elektrického vedení na Liberecku a na Frýdlantsku. Nové vedení velmi vysokého napětí za 100 milionů korun povede ke zvýšení spolehlivosti dodávek i k větší stabilitě distribuční soustavy. Strategická stavba dvojitého vedení velmi vysokého napětí 110 kV na trase Bezděčín - Šimonovice s sebou nesla řadu úskalí. Prochází obtížným zalesněným a kopcovitým terénem. Vedení je na území Přírodního parku Ještěd, část trasy je v chráněné oblasti přirozené akumulace vod. Prochází také ochranným pásmem neelektrifikované železniční tratě Turnov - Liberec, ve třech případech tuto trať křižuje. Projekt se připravoval od roku 2006, vlastní zahájení zdržovala komplikovaná majetkoprávní vypořádání s majiteli pozemků. Samotná stavba 8 350 metrů dlouhého dvojvedení se 37 stožáry pak trvala od května do prosince 2013.

Silný mráz a polámané stromy připravily Velké Meziříčí o dodávky proudu

Velké problémy způsobil 19. prosince příchod zimního počasí energetikům na Vysočině, kde silná námraza poškodila elektrické vedení. Bez elektřiny se tak ocitla většina z téměř 12 tisíc obyvatel Velkého Meziříčí. Mluvčí společnosti E.ON Vladimír Vácha ČTK řekl, že vodiče byly poškozeny, přestože je energetici vyhřívali.

V Tanvaldu má vzniknout nová geotermální elektrárna

Společnost Entergeo připravuje výstavbu nové geotermální elektrárny v areálu zkrachovalé textilní továrny v Tanvaldu. Zařízení by mělo vhánět vodu do podzemí a odtud ji ohřátou čerpat zpět na povrch. Panují nicméně obavy z málo prověřené technologie, která v zahraničí (např. v Německu) způsobila silné otřesy. Ve švýcarské Basileji bylo kvůli nim nutné dokonce projekt zcela zastavit.

Německo plánuje stavbu nových vedení do Česka, Polska i Skandinávie
Německý provozovatel přenosových sítí Herz50 plánuje stavbu nových vedení do Česka, Polska, Dánska a Švédska. Pomocí nich chce do zahraničí prodávat přebytkovou elektřinu z obnovitelných zdrojů a zvýšit stabilitu přenosové soustavy v regionu, kterou nadbytek proudu v Německu a jeho nekontrolované přetoky přes hranice narušují. Napsal to dnes německý deník Frankfurter Allgemeine Zeitung (FAZ), podle něhož jsou příslušné smlouvy s Českem a Polskem krátce před podpisem. Souběžně s opatřeními v Česku a Polsku plánuje 50Herz výstavbu nových podmořských kabelů do Skandinávie, které mají umožnit prodávat Seveřanům přebytkovou elektřinu z německých větrných elektráren v době, kdy tamní vodní elektrárny neprodukují dostatek proudu.

Mrazy v USA způsobily rozsáhlé blackouty
Několik milionů lidí se ve Spojených státech ocitlo bez dodávek elektrické energie kvůli velké vlně mrazů a sněhových bouří, které si mj. vyžádaly také přes 20 obětí. Nejhorší situace byla podle místních úřadů ve státě Oklahoma. Bez elektřiny tam zůstalo přes půl milionu odběratelů. "Co do počtu postižených domácností je tato ledová bouře nejhorší, jakou jsme v historii naší společnosti zažili," řekl Brian Alford, mluvčí oklahomské plynárenské a elektrárenské společnosti. Jeho kolega Gil Broyles v rozhovoru z 11. prosince dodal: „Pravděpodobně jeden ze tří obyvatel Oklahomy nemá v tuto chvíli elektřinu."
Pod tíhou sněhu a ledu se trhala elektrická vedení, strhávaly je také padající stromy. Po celém území státu se otevřely útulky pro lidi, které z jejich domů vyhnala tma a zima. Obnovení dodávek trvalo v některých místech energetikům až týden. V Missouri bylo bez elektřiny na 100 000 odběratelů, ve státě byl vyhlášen stav nouze. V některých oblastech se vytvořila ledová námraza o tloušťce dva a půl centimetru, která trhala dráty elektrického vedení. V Illinois bylo bez proudu 11 000 domácností a v Kansasu 5 000.
Kvůli energetickým výpadkům a mrazům musely být zrušeny také stovky letů. Například letiště v Tulse bylo deset hodin mimo provoz, protože bylo odříznuté od elektřiny.

Zdroje pro tuto kapitolu: MV, MPO, vlada.cz, prumysl.cz, ČT24, lidovky.cz, novinky.cz, ppas.cz, ceps.cz, cez.cz, ceskatelevize.cz, akualne.cz, idnes.cz, enviweb.cz, tretiruka.cz, ceskenoviny.cz, rozhlas.cz, reko a.s., e15.cz, euraktiv.cz, atominfo.cz, ČTK, novinky.cz, PČR, GŘ HZS ČR, sxc.hu, govcert.cz, spiegel.de, bihdaytonproject.com, eon.cz, elektrika.cz

BEZPEČNOST FINANČNÍCH INSTITUCÍ

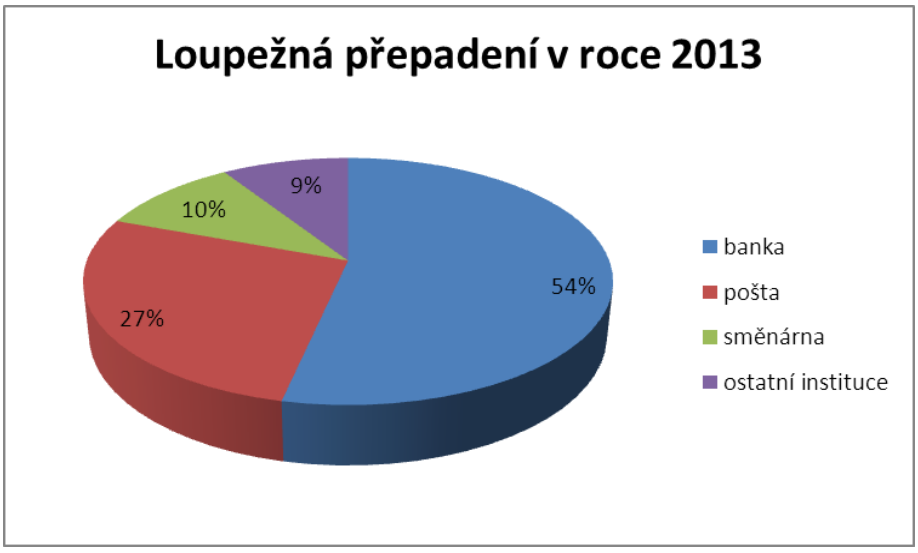
Policejní statistiky a jejich interpretace

Trestná činnost související s finančními institucemi je značně rozmanitá a zahrnuje množství skutkových podstat. V této kapitole se nejdříve v policejních statistikách zaměříme na ty nejdramatičtější, a sice **loupeže**. Následovat budou další formy trestné činnosti od skimmingu, přes úvěrové a pojistné podvody. Nakonec věnujeme delší exkurz fenoménu, který jsme v Situační zprávě dosud nezpracovávali – padělání platidel. Zdrojem všech tabulek a grafů, uvedených v této části, je Policie České republiky.

loupežná přepadení (§ 173 Loupež z. č. 40/2009 Sb.) finančních institucí za období leden až prosinec 2013

registrované skutky	88
počet skutků, u nichž byl zjištěn pachatel	50
škoda	5 003 500 Kč

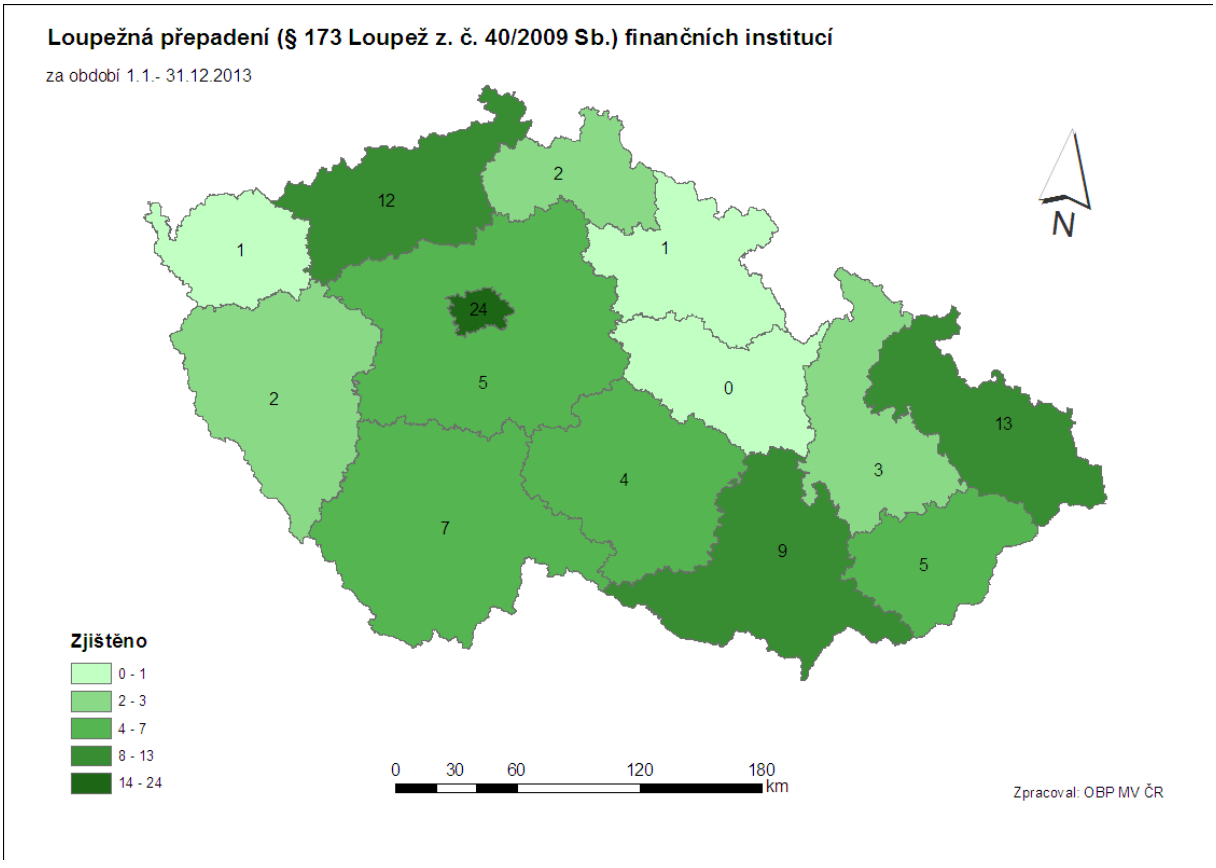
Jak vyplývá z výše uvedené tabulky, každý měsíc v roce dojde v České republice v průměru k sedmi loupežím. Jak lze vidět na následujícím grafu, nejčastější obětí jsou banky, následují pošty a směnárny. Objasněnost těchto činů policií je přitom značná, **pachatel je ještě tentýž rok dopaden v 57% případů** (v dlouhodobém časovém horizontu je policie ještě úspěšnější).



Tato forma trestné činnosti v posledních letech nijak dramaticky neroste, naopak byl zaznamenán mírný pokles. Loupežná přepadení finanční institucí jsou páchána osobami, které se rekrutují především z řad neúspěšných podnikatelů či osob, pociťujících stále větší nedostatek finančních prostředků. Tito lidé i přesto, že vědí o bezpečnostních opatřeních v jednotlivých pobočkách finančních ústavů, riskují, že budou zachyceni bezpečnostními systémy a při následném vyšetřování poznáni zaměstnanci bank či svědky.

Loupežná přepadení v bankách jsou páchána především jednotlivci, kteří většinou zbraň nebo její maketu užijí jen k zastrašení. K jejímu skutečnému použití dochází jen ve výjimečných případech. Páchání těchto skutků **často překračuje rámec jednoho kraje a má sériový charakter**. Z těchto důvodů Úřad služby kriminální policie a vyšetřování přijal opatření ke zlepšení koordinační činnosti směrem k jednotlivým útvarům s cílem zmapovat, porovnat a vyhodnotit užitý modus operandi jednotlivých skutků zapadajících do série loupežných přepadení. Cílem je zlepšení vzájemné komunikace a kooperace při objasňování této závažné násilné trestné činnosti. V rámci neustálého prohlubování vztahů s civilním sektorem je zintenzivňována i spolupráce především s pracovníky Bezpečnostní komise České bankovní asociace. Předmětem této spolupráce je zejména vzájemná výměna informací a součinnost při zavádění nových technologií do ochrany jednotlivých poboček.

Jak je vidět na připojené mapce, zdaleka nejvíce se loupí v Praze (27% případů). Teprve s velkým odstupem následují v počtu loupežných přepadení kraje Moravskoslezský a Ústecký, kde je **incidence oproti Praze poloviční, třebaže mají srovnatelný počet obyvatel**. O tom, že počet přepadení s lidnatostí přímo nekoreluje, svědčí relativně nízký počet těchto incidentů v Jihomoravském kraji a Středočeském kraji. Relativně horší ekonomická situace občanů na severu Moravy a severozápadě Čech tak zřejmě přispívá k nárůstu výskytu tohoto typu trestné činnosti v těchto oblastech. Případ Prahy je pochopitelně specifický a je dán jejím metropolitním charakterem (velké město přispívá k anonymitě pachatelů, ti také často předpokládají, že zde pobočky bank disponují větší hotovostí).



V předchozích Situačních zprávách (a tato nebude výjimkou), jsme se hodně věnovali trestným činům, kde byl předmětem zájmu pachatelů bankomat (nejčastěji to byl **fenomén skimmingu**). Jejich celkový počet a úspěšnost policie při jejich objasňování v průběhu uplynulého roku shrnuje následující tabulka:

trestné činy, kdy předmětem zájmu byl bankomat
za období leden až prosinec 2013

registrované skutky	36
počet skutků, u nichž byl zjištěn pachatel	9
škoda	3 864 100 Kč

Skutečný počet napadených bankomatů je nicméně vyšší. Do výše uvedené statistiky se započítávají jen trestné činy (v tomto případě krádež, poškození cizí věci a výtržnictví). Pokud započítáme i skutky, které nejsou trestným činem, tak bylo o rok dříve, tj. v roce 2012 v České republice napadeno celkem 150 bankomatů, z toho 114 na území Prahy. V roce 2013 začalo být nicméně dominantní postavení metropole narušováno a tato činnost se ve stále větší míře **přesouvá do regionů**. Důvodem je zejména lepší práce policie, jejíž úspěšnost při odhalování skimmingu v Praze stále roste (v Praze již přesáhla 50%). Naopak v menších městech zkušenosti s touto formou trestné činnosti chybí, a proto se pozornost pachatelů nově ubírá právě tam.

V uplynulém roce začali nicméně zloději **používat nový trik pro zkopírování dat z kreditní karty**. Jde o tenký, na první pohled téměř neviditelný pásek, kteří pachatelé vyvinuli speciálně pro bankomaty vybavené zelenou vstupní čtečkou (tzv. „zelenou žábou“), kterou přitom banky instalují právě kvůli ztížení skimmingu. Asi pět centimetrů dlouhý proužek, zatavený v zeleném plastu (tedy v barvě čtečky), zloději vlepí do otvoru na kartu a tím mohou zkopírovat údaje z magnetického proužku karty. Set s minikamerou, kterou pachatelé rovněž potřebují pro získání PINu, je vyjde jen asi na tisíc euro.

Zařízení sloužící ke zkopírování karet přitom vůbec nemusí být v samotném bankomatu. Objevily se i případy, kdy ho pachatel nainstaloval do čtečky ve dveřích banky, kterou zákazníci používají, když si jsou vybrat své peníze v nočních hodinách. Také miniaturní kamera nemusí být umístěna přímo na bankomatu, ale např. v požárním hlásiči na stropě. Velké množství lidí totiž stále při zadávání PINu nezakrývá klávesnici rukou, případně tak činí velmi nedůsledně.

Zdá se, že pachatelé se nesoustředí na zařízení žádné konkrétní banky, ale svou pozornost rovnoměrně věnují bankomatům všech finančních ústavů. Napadené bankomaty se také nacházely v různých částech měst, zvláštní oblíbenosti se ale těší ty v centru Prahy, kde si své peníze vybírají mnohdy nepozorní turisté (čestné první místo v počtu napadení drží bankomat na Národní třídě).

Skimming je obvykle záležitostí **mezinárodních organizovaných skupin**. Samotnou instalaci skimmovacích zařízení (tedy nejrizikovější díl práce gangu) zajišťují v České republice mnohdy cizinci, většinou občané některé ze zemí Balkánu, vůbec nejčastěji z Bulharska (kde také podle některých zdrojů skimming vznikl). Peníze ze zkopírovaných karet se ovšem většinou vybírají v zámoří (Dominikánská republika, Keňa, Peru, často také USA, zejména Chicago). V Evropě totiž bankomaty většinou čtou údaje z čipu, jehož okopírování je výrazně složitější. V mimoevropských zemích ovšem bankomaty často pracují jen s magnetickým proužkem, údaje o něm pak pachatelé z ČR snadno zašlou v digitální podobě svým komplicům na jiný kontinent. Často se jim tak podaří ilegálně získat až několik milionů korun (ve většině případů jsou to ale stovky tisíc z jednoho napadeného bankomatu). Pachatelé působící v ČR pak získají jen zlomek této částky (obvykle pětinu), což svědčí o tom, že pro tuto činnost jsou využíváni lidé, stojící na nižších příčkách žebříčku v hierarchii organizovaných skupin (v případě dopadení tito lidé často vůbec netuší, kdo je vlastně členem zámořské části gangu a jak celá skupina funguje).

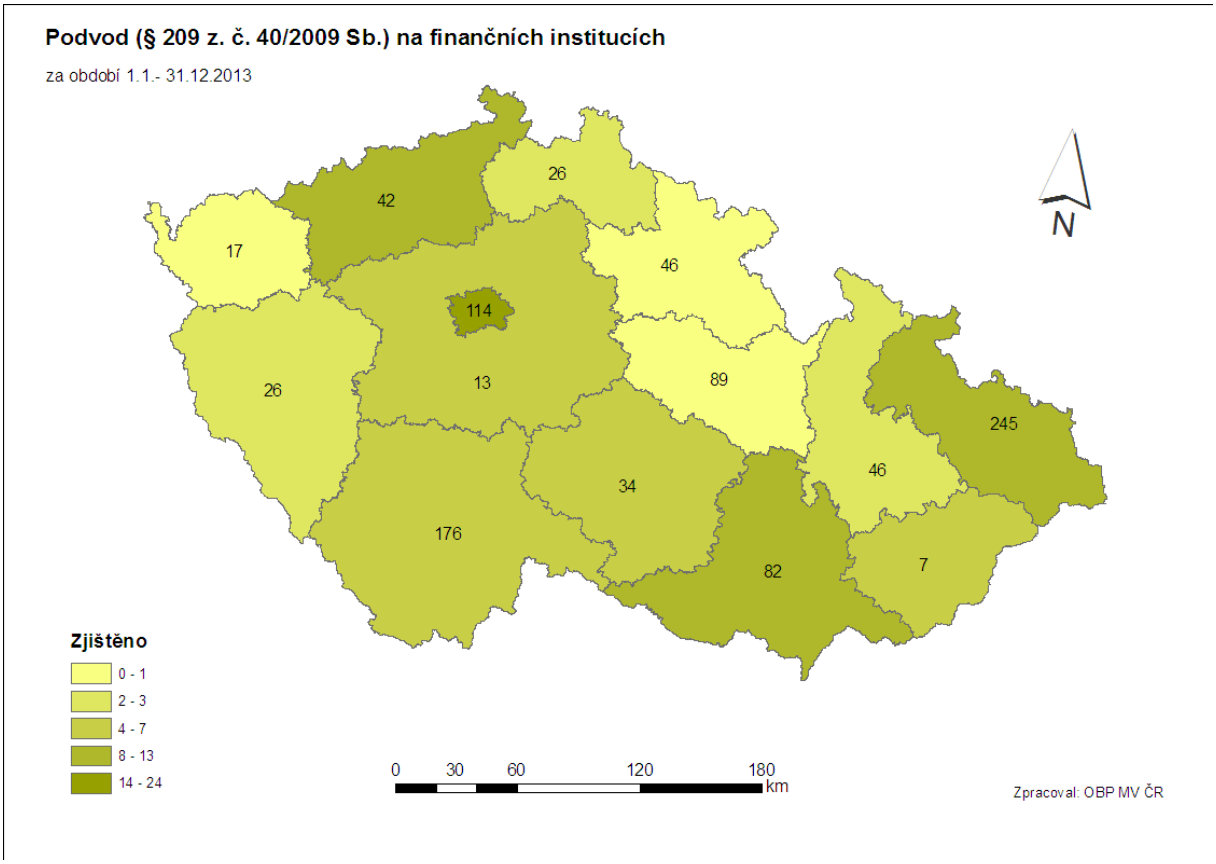
Samotné banky se snaží proti skimmingu bojovat také tím, že **monitorují podezřelé transakce** (výběr mimořádně velkého objemu peněž v rizikových zemích) a uvědomí jejich majitele, případně kartu rovnou zablokují. Zvažuje se také zcela nový způsob ochrany – magnetické pole, které veškerá případná skimmovací zařízení vyřadí z provozu. Věčný souboj majitelů bankomatů a pachatelů skimmingu tak zřejmě čekají další dějství.

V další části se zaměříme na **trestné činy podvodu** (podle §209 Trestního zákoníku), který si pro přehlednost zúžíme pouze na objekt hospodářské kriminality (a pomineme kriminalitu obecnou). Počet těchto skutků přehledně znázorňuje následující tabulka:

podvod (§ 209 z. č. 40/2009 Sb.) na finančních institucích
objekt hospodářské kriminality za období leden až prosinec 2013

registrované skutky	963
počet skutků, u nichž byl zjištěn pachatel	718
škoda	335 666 200 Kč

Co se týče geografického rozložení, pak se v tomto případě jedná o jeden z mála trestných činů, ve kterém nevévodí Praha (ta je se 114 spáchanými skutky za rok 2013 dokonce až na třetím místě). Jasně první místo v tomto ohledu drží kraj Moravskoslezský (245 případů), následován překvapivě krajem Jihočeským (159 případů).



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

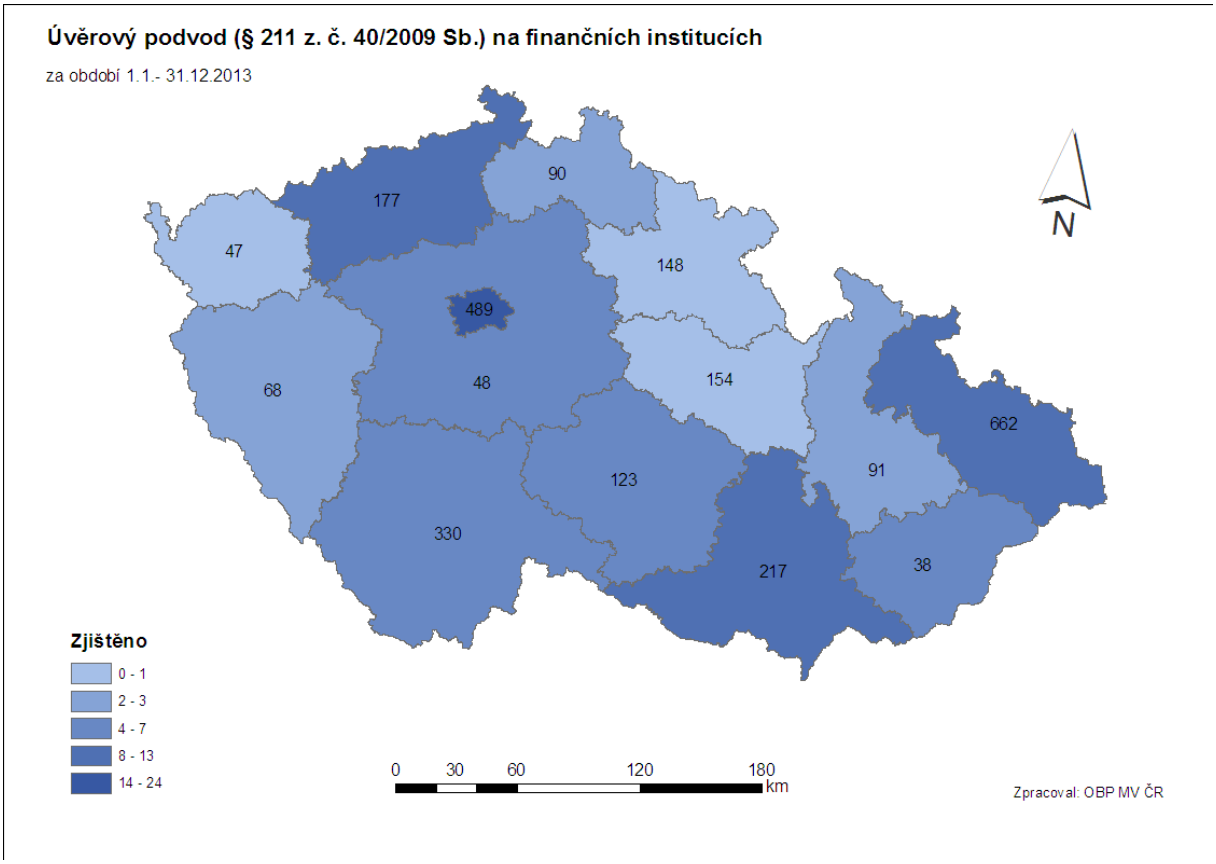
úvěrový podvod (§ 211 z. č. 40/2009 Sb.) na finančních institucích
objekt hospodářské kriminality za období leden až prosinec 2013

registrované skutky	2 682
počet skutků, u nichž byl zjištěn pachatel	2 166
škoda	1 833 240 900 Kč

Kriminalita v oblasti **úvěrových podvodů** je v roce 2013 výrazně vzrůstající v porovnání se stejným obdobím roku loňského. Vyčíslená škoda za delikty spáchané v této oblasti je za rok

2013 výrazně vyšší (téměř dvě miliardy Kč). **Objasněnost úvěrových podvodů** se oproti roku 2012 pohybuje na nepatrně vyšší úrovni, tedy **na 83,6 %**.

Důvody nárůstu této trestné činnosti jsou spatřovány především v horší ekonomické situaci v ČR, větší zadluženosti občanů ČR a nutnosti získání dodatečných finančních prostředků. Dochází ke konsolidaci půjček a tedy uzavírání nových úvěrových smluv, z čehož lze dovozovat udržování míry objemu těchto produktů bankami na vyšší úrovni než v loňském roce. Míra vzniklých škod je vyšší z důvodu nárůstu objemu poskytnutých úvěrů především nebankovním sektorem. Tento stav samozřejmě úzce souvisí s neuspokojivou finanční situací a nezaměstnaností občanů v jednotlivých regionech. Zřejmě tento fakt stojí za počtem zaznamenaných úvěrových podvodů, tak jak je znázorňuje následující mapa:



Významnou měrou je totiž dle aktuální statistiky pachatelem úvěrového podvodu nezaměstnaný, důchodce příp. invalidní důchodce, přičemž **jednotlivá částka úvěru** (poskytnutého nejrůznějšími společnostmi, které úvěr poskytují, nikoli velkými bankovními domy) **nepřesahuje částku pět nebo deset tisíc Kč**, avšak pachatel si vezme takovéto úvěry i čtyři, u různých společností, aby z prvních dvou splatil úvěr předešlý a další dva má na pokrytí nutných výdajů (inkasní poplatky, elektřina, apod.). Aby úvěr získal, v žádosti nejčastěji uvede nepravdivý údaj o „zaměstnavateli“ a výši mzdy, případně o výši důchodu nebo příjmu z brigády, a následně úvěr nesplácí.

Stejný modus operandi, tedy uvedení nepravdivých údajů v žádosti o poskytnutí úvěru, je používán i v případě úvěrů spotřebitelských, poskytovaných na vybavení domácnosti. Další skupinou pachatelů v rámci celé ČR, jsou osoby, které získají úvěr v řádu statisíců až milionů Kč na základě odcizených nebo padělaných dokladů totožnosti a padělaných listin, vyžadovaných bankou za účelem ověření klienta a jeho schopnosti úvěr splácet (nejčastěji padělaná daňová přiznání, potvrzení FÚ a sociální správy o bezdlužnosti, prohlášení o ročním obratu firmy aj). Tyto úvěrové podvody jsou páchány velmi sofistikovaně, zjištění pachatele je náročné, přičemž je zřejmé, že se již nejedná o trestnou činnost páchanou ze sociálních důvodů, ale s cílem rychlého

obohacení se (pachateli a organizátory jsou nezřídka středoškolsky a vysokoškolsky vzdělané osoby). Trendem pro rok 2014 zůstává nárůst počtu spáchaných úvěrových podvodů (v porovnání s rokem 2013).

Nejen banky, ale také **pojišťovny jsou častým terčem trestné činnosti**. Zde je přehled nejčastějších trestných činů, které trápí pojišťovací ústavy:

trestné činy, kdy objektem hospodářské kriminality byla pojišťovna za období leden až prosinec 2013

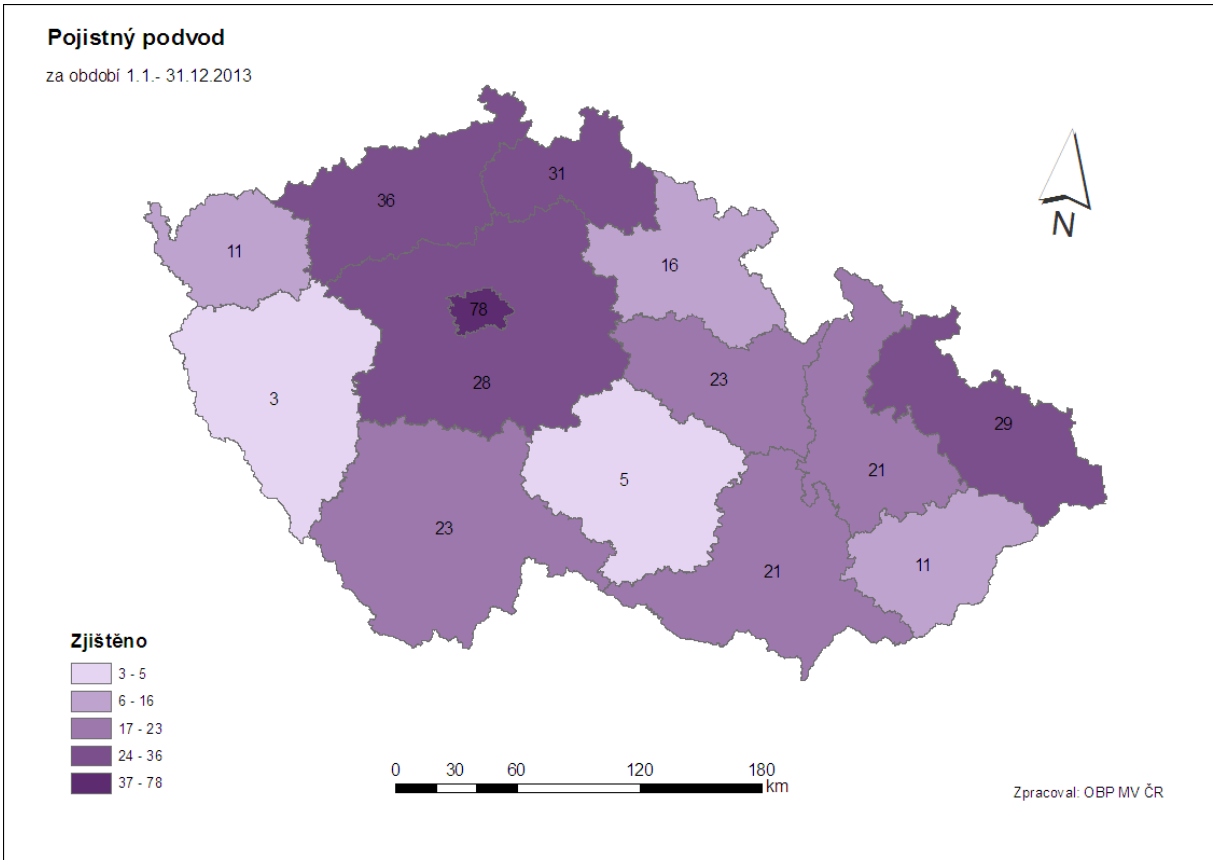
	§ 206 Zpronevěra	§ 209 Podvod	§ 210 Pojistný podvod	§ 211 Úvěrový podvod	§ 220 Porušení povinnosti při správě cizího majetku
registrované skutky	13	105	336	4	2
počet skutků, u nichž byl zjištěn pachatel	10	83	214	3	0
škoda	6 646 800 Kč	53 827 700 Kč	37 718 400 Kč	280 000 Kč	150 975 100 Kč

§ 221 Poruš. povin. při správě cizího majetku z nedbalosti	§ 222 Poškození věřitele	§ 223 Zvýhodnění věřitele	§ 241 Neodved. daně, pojist. na soc. zabezp.	§ 254 Zkreslování údajů o stavu hospodaření a jmění	§ 329 Zneužití pravomoci úřední osoby
1	3	2	97	3	1
1	2	2	70	3	1
1 046 900 Kč	923 200 Kč	138 500 Kč	19 635 600 Kč	824 600 Kč	0 Kč

V následujících několika odstavcích se zaměříme na otázku **pojistných podvodů**. Kriminalita v oblasti pojistných podvodů ani v roce 2013 nenabízí významné rozdíly mezi hodnocenými obdobími s rokem 2012. **V roce 2013 bylo spácháno skoro stejně skutků**. Vyčíslená škoda za delikty spáchané v této oblasti je za rok 2013 oproti roku 2012 nižší. I přesto lze konstatovat, že se nadále celková částka vzniklých škod udržuje na vysoké úrovni. Počet zjištěných trestných činů pojistného podvodu se v roce 2013 nepatrně snížil. V porovnání s rokem 2012 je hranice téměř shodná. Objem těchto spáchaných trestných činů ale zdaleka nedosahuje takového počtu, jako u podvodů úvěrových. **Objasněnost pojistných podvodů se pohybuje na přibližně stejné úrovni jako v roce 2012**. Dlouhodobý trend páchání pojistných podvodů je v počtu všech spáchaných skutků stabilizovaný.

V rámci problematiky jsou stále zaznamenávány jako nejčetnější pojistné podvody v souvislosti s pojištěním vozidel, avšak na vzestupu jsou také pojistné podvody v souvislosti s pojištěním osob. Jejich zjišťování a objasňování však patří mezi ty složitější, a proto je na místě i v roce 2014 zaujmout větší pozornost těmto formám páchání trestné činnosti.

Oblasti pojistných podvodů opět jasně vévodí Praha (78 policií evidovaných případů za rok 2013), následovaná Ústeckým (36) a Libereckým krajem (31 případů). Velmi nízký byl tentokrát počet pojistných podvodů v kraji Plzeňském (pouze 3). Přehledně incidenci znázorňuje mapa:



Vysoký počet pojistných podvodů na severu Čech může souviset s povodněmi v první části roku. Je všeobecně známým jevem, že **v čase velkých živelných katastrof narůstá počet snah o pojistné podvody**. Pojišťovny totiž musí řešit velký počet pojistných událostí a pachatelé se domnívají, že pak jednotlivé případy prošetřují s menší pečlivostí. Ve skutečnosti je tomu ale spíše naopak.

Ne vždy se ovšem jedná o události zcela vymyšlené, spíše se někteří lidé snaží na své skutečné škodě vydělat více, než by jim správně náleželo. Nezřídka tak dochází k tomu, že vytopené domácnosti požadují proplacení drahých předmětů, které nikdy nevlastnily atd. Na severu Čech například muž nahlásil, že mu voda v soukromé garáži odnesla tak velký počet nářadí, že by si s ním vystačil i středně velký obchod pro kutily. V jiném případě měla zase údajně odplavat celá kuchyně oknem, kterým by se stěží protáhlo dítě.

Detektivové pojišťoven nemají vůbec lehkou úlohu. Podle některých odhadů celkově pojišťovny vyplatí až 10% plnění, na které lidé ve skutečnosti nemají nárok. Celkový objem pojistných podvodů tak může teoreticky jít až do výše miliard korun. Objasněnost se nicméně neustále zvyšuje, stejně jako **jsou proti podvodníkům užívány stále sofistikovanější metody**. Některé pojišťovny například nakoupily hlasové analyzátory, které používají v případě, že poškozený nahlašuje pojistnou událost přes telefon. Toto zařízení odhalí lživé tvrzení s údajně pozoruhodnou přesností.

Fenomén: padělání platidel

Spojené státy i Evropská unie vydávají nové série bankovek, které mají být odolnější vůči padělání. V této souvislosti přinášíme krátký exkurz, zabývající se fenoménem falšování bankovek a mincí v České republice. Podíváme se na vývoj počtu zadržených padělků v několika posledních letech, zjistíme, jak zdatní jsou čeští padělatelé, a doporučíme několik základních tipů, jak poznat falešnou bankovku od pravé.

Padělání peněz v ČR

Česká národní banka vydává pravidelně koncem února výroční zprávu o počtu a hodnotě zachycených falešných mincí a bankovek. **V České republice je každoročně zadrženo v průměru 4000 – 6000 kusů padělaného oběživa různých měn**.

Jak ukazuje následující graf, docházelo až do roku 2010 k poměrně rychlému nárůstu počtu falešných peněz (je možné, že za touto skutečností stojí nástup finanční krize), tento **negativní trend se ale podařilo v posledních dvou letech zvrátit**. Protože souhrnná zpráva za rok 2013 dosud není k dispozici, není zatím zřejmé, zdali došlo k dalšímu poklesu i v roce právě minulém, průběžná čísla tomu ovšem nasvědčovala.

Jak je z grafu jasně patrné, padělky českých měn pravidelně vysoce převažují nad zadrženými padělky měn zahraničních. Výjimkou byl rok 2009, kdy se jejich počet téměř vyrovnal. Důvodem byl tehdy především velmi úspěšný zásah policejního Útvaru pro odhalování organizovaného zločinu, při kterém se podařilo **rozbít část mezinárodní sítě padělatelů eurobankovek** a bylo zadrženo více než 1900 kusů stoeurových padělků.

Trojici Italů a jednoho Čecha tehdy zadržel Útvar rychlého nasazení před brněnským centrem Olympia. Padělatelská dílna se nicméně na českém území nenacházela, přes Českou republiku se mezinárodní gang pouze snažil uvádět falešná eura do oběhu. U kvalitnějších padělků totiž není mezistátní spolupráce pachatelů nijak výjimečným jevem. Svědčí o tom například jeden z největších případů padělání z konce 90. let, kdy nelegální dílna na Moravě produkovala velké množství maďarských forintů.

Jak si ovšem ukážeme vzápětí, kvalitní padělky české měny, které jsou dílem organizovaných skupin, jsou v posledních letech spíše výjimkou. Svou roli v tom hraje i fakt, že česká koruna je v oblasti padělání obecně považována bezpečnou, a to i v mezinárodním srovnání. Například v poměru k celkovému počtu oběživa **se české bankovky padělají zhruba 7x méně než eura**, vůči americkým dolarům je tento poměr dle odhadů dokonce ještě příznivější. V průměru připadá jeden padělek české měny na více než 100 000 pravých bankovek, proto se s ním v běžném životě setká jen velice málo občanů.

Jak poznat falešné peníze

Většina padělků, se kterými se v ČR můžete setkat, je nekvalitních a obvykle se dají při troše pozornosti dobře rozeznat. Stačí k tomu 3 jednoduché kroky. Nejprve bankovku promněte v prstech – jen málo padělatelů je schopno dobře napodobit kvalitu a typ papíru, který používá Státní tiskárna cenin. Pohledem na bankovku proti světlu zase ověříte, že nechybí vodoznak, dávejte pozor také na celkový barevný odstín. Při naklonění bankovky zkontrolujte bezpečnostní proužek a další ochranné prvky. U euromincí je zase možné kontrolovat jejich pravost pomocí magnetu. Obsahují totiž malé množství niklu, takže jsou mírně magnetické, ale z magnetu snadno sklepnutelné. Padělky většinou magnet vůbec nepřitahuje, anebo z něj naopak nejdou sklepnout.

V roce 2007 až 2009 provedla Česká národní banka další úpravy vzhledu a doplnění nových ochranných prvků českých bankovek, které jsou teď vůči padělání ještě odolnější. I v důsledku těchto opatření patří česká měna ve světě mezi ta platidla, která pachatele k padělání příliš nesvádí (pozitivní roli zde pochopitelně hraje i její relativně menší rozšíření než např. v případě eur, dolarů či rublů).

Padělky zadržené v posledních několika letech se **obecně vyznačují velice nízkou kvalitou**, obvykle se jedná o práci amatérů, kteří si „zkusí“ vytisknout několik kusů nepříliš zdařilých napodobenin, se kterými se pak pokouší zaplatit. Kupodivu se jim to občas podaří, což svědčí o tom, že lidé při placení nevěnují stavu bankovek příliš velkou pozornost. Falešné mince či bankovky pak často odhalí až pošta či banka.

Česká národní banka rozlišuje pět stupňů kvality padělků. Falešné bankovky a mince stupně jedna jsou nejkvalitnější a nejnebezpečnější – od originálu je rozezná jen odborník. Dobrou zprávou ovšem je, že **padělek české měny stupně jedna se naposledy objevil v roce 2005**. Ve skutečnosti většinou **výrazně převažují padělky stupňů čtyři až pět** (těch je 90%), které by měl bez větších potíží rozeznat i naprostý laik. V těchto případech totiž pachatelé obvykle k jejich výrobě používají běžné barevné tiskárny či kopírky, na kterých se pochopitelně kvalitní falešná bankovka ani vyrobit nedá.

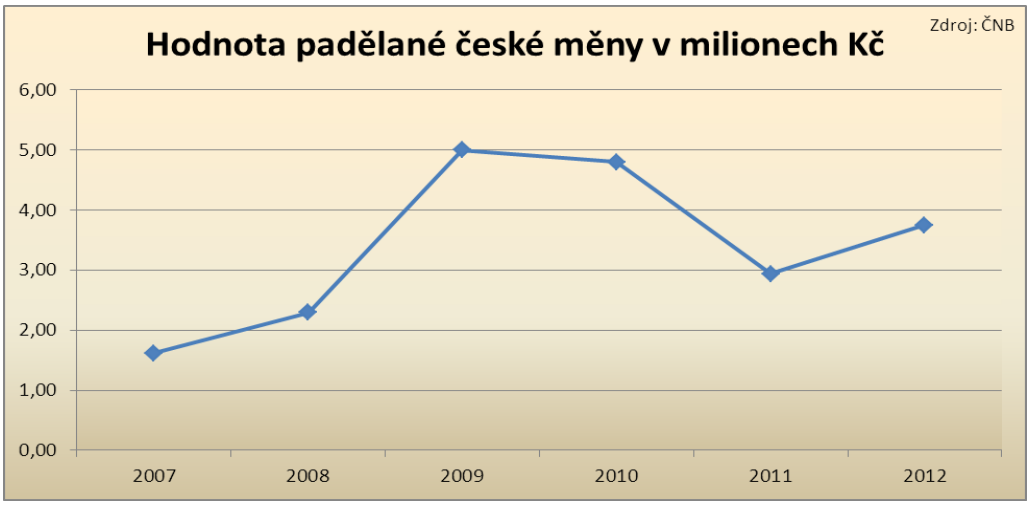
Jeden z typických případů se odehrál v květnu 2013 na Chrudimsku. Detektivové z pardubické hospodářské kriminálky zde zadrželi dva muže ve věku 35 a 27 let. Ti vyráběli padělky na tiskárně, kterou koupili za pouhých 999 korun. Tyto napodobeniny byly pochopitelně značně nekvalitní, přesto se jich podařilo několik desítek dostat do oběhu. Oba muži přitom využívali zejména lidské nepozornosti. Pachatelé totiž zkoušejí různé triky, jak padělanými bankovkami zaplatit. Nepokouší se je většinou udat v bankách či na poštách, kde je velké riziko odhalení – vůbec nejlepším terčem jsou zdá se pouliční trafiky, kde prodavači kvůli špatnému výhledu z okénka bankovky i zákazníka hůře rozpoznávají. Falešné bankovky jsou také často při placení přimíchány mezi ty pravé. Několik tipů jak poznat falešnou bankovku naleznete v textu v rámečku.

Je pozoruhodné, že se tyto pokusy nepřestávají objevovat navzdory tomu, že amatérské padělání je jedním z nejméně „rentabilních“ druhů zločinu. Velmi zřídka se podaří uvést do oběhu tak velké množství falešných bankovek, aby se zločincům vyplatilo riskovat, objasněnost těchto případů ze strany policie je totiž poměrně vysoká. Za tuto činnost navíc

hrozí dosti vysoké tresty – **za padělání platidel můžete ve vězení strávit od tří do osmi let** (přihlíží se přitom k tomu, zda byli pachatelé součástí organizované skupiny či nikoliv).

Pokud člověk zjistí, že se mu dostala do ruky padělaná bankovka či mince jakékoliv měny, musí ji odevzdat na policii. Přijmout v nevědomosti falešné platidlo není trestné, bude pouze nutné podat policistům vysvětlení, kde a kdy k tomu zřejmě došlo. Za odevzdané falešné peníze nicméně nevzniká nárok na žádné finanční odškodnění, jak se někteří lidé mylně domnívají. Za mimořádně špatný nápad je ovšem možné označit snahu „udat" padělek dál. Vědomé placení s falešnými penězi již trestným činem je a i v případě, že sami nejste tvůrcem padělku, vám za takový pokus hrozí až dva roky vězení.

Jak je patrné z následujícího grafu, nominální hodnota zadržených padělků rok od roku kolísá, dosavadního maxima dosáhla v roce 2009, kdy byly zadrženy falešné mince a bankovky v hodnotě téměř 5 milionů korun.



Počty zadržených mincí a bankovek různých měn za rok 2012 je možné vidět na následující tabulce. Aktuální data pro rok 2013 bude možné nalézt na konci února na stránkách České národní banky (www.cnb.cz).

	Zadrženo		
	v oběhu	policií	celkem
Padělané bankovky CZK	2 612	845	**3 457**
Padělané bankovky EUR	572	73	**645**
Padělané bankovky USD	131	0	**131**
Padělané bankovky ostatní	68	0	**68**
Padělané mince CZK	113	0	**113**
Padělané mince ostatní	82	0	**82**
Pozměněné bankovky a mince CZK	16	0	**16**
Pozměněné bankovky a mince ostatní	2	0	**2**
Celkem	**3 596**	**918**	**4 514**

Nová eura a dolary

Jak již bylo řečeno, **česká měna bývá v mezinárodních srovnáních hodnocena jako velmi bezpečná**. Naopak jednou z nejpadělanějších měn zůstává americký dolar, což je dáno jednak jeho klíčovou rolí v globálním finančním systému, ale také relativně konzervativním přístupem, který Spojené státy uplatňují k zavádění nových bezpečnostních prvků. Jeho podoba má totiž oproti řadě jiných měn delší tradici, například současný design jednodolarových bankovek se používá již od roku 1964.

Vyšší počet padělků nicméně v říjnu 2013 přiměl americkou centrální banku (FED) k vydání nové série stodolarových bankovek, která tyto bezpečnostní deficity smazává. Tato nominální hodnota přitom patřila mezi padělateli k nejoblíbenějším. Bankovka obsahuje několik důležitých novinek – měnící se barvu tisku, vodoznak, mikrotisk na límci Benjamina Franklina atd. Novou součástí bankovky je také část textu Deklarace nezávislosti.

Nový design bankovky byl zveřejněn už v roce 2010, kvůli problémům při výrobním postupu byly ale do oběhu uvedeny až nyní. Podobným způsobem byly již vylepšeny bankovky v hodnotě 5, 10, 20 a 50 dolarů, pouze legendární jednodolarovka zůstává stále beze změny.

Také Evropská unie se snaží čelit padělatelům posilováním bezpečnostních prvků svých bankovek. **Po nové pětieurovce přichází počátkem roku 2014 nová desetieurová bankovka s vylepšenou ochranou**. Následovat budou brzy i všechny další eurobankovky vyšších hodnot. Součástí desetieurových bankovek nové série je podobizna Európy, postavy z řecké mytologie, od které je odvozen i název světadílu. Ta je vyznačena na hologramu a ve vodoznaku. Jinak je design velmi podobný tomu předchozímu.

Číslo označující nominální hodnotu bude nyní při naklonění měnit barvu, k dispozici budou i další bezpečnostní prvky. Nové unijní bankovky budou také šetrnější k životnímu prostředí, neboť díky vylepšené ochranné vrstvě déle vydrží a nebude je nutné tak často obměňovat. V současné době **je v oběhu asi 15 miliard eurobankovek v celkové hodnotě 900 miliard eur**. Ve druhé polovině roku 2013 bylo přitom zadrženo celkem 353 tisíc padělků, což je o 11,4% více, než v předchozím pololetí. Nejvíce se falšují bankovky v hodnotě 20 a 50 EUR (78% padělků), naopak nejméně je mezi zločinci paradoxně oblíbená bankovka nejvyšší hodnoty 500 EUR (jen 1% padělků). Ta je totiž mimo bankovní domy jen těžko uplatnitelná.

Drtivá **většina padělků byla odhalena v zemích eurozóny (98%)**, jen asi 1,5% pak bylo nalezeno v těch zemích unie, kde se eurem neplatí (sem patří i Česká republika). Asi 0,5% padělků unijní měny se zadrží mimo její hranice. Celkově počet padělaných eur, na rozdíl od českých korun, každoročně stoupá.

Vybrané události ve sledovaném období

Červenec

Policisté odhalili pachatele jednoho nejrozsáhlejších případů skimmingu v Čechách

Tři cizinci, kteří nainstalovali elektronické skimmovací zařízení na bankomat v Blatné na Strakonicku, zadrželi jihočeští kriminalisté. Spolu s 36letým a 40letým Rumunem a třicetiletým Bulharem se podařilo policejním specialistům zajistit i padělatelské náčiní. Podle dosavadního vyšetřování jde o nejrozsáhlejší případ skimmingu vyšetřovaný kriminalisty na jihu Čech. Na stopu pachatelů je přivedl 32letý muž, který se pokusil z bankomatu v Blatné minulé úterý vybrat peníze.
"Zasunul kartu do přístroje, ta se v něm však zasekla a nešla ven. Muž proto kartu násilím vytrhl. Nestačil se divit, když mu kromě ní v ruce zůstalo i nezákonné čtecí zařízení, které nevědomky oddělil od bankomatu. Proto se ihned obrátil na policii," popsala jihočeská policejní mluvčí Štěpánka Uhlířová. Na místo přijeli strakoničtí kriminalisté, kteří spolu s krajskými kolegy začali na případu pracovat. Podařilo se jim sehnat popis tří mužů, kteří zařízení nainstalovali na bankomat jen několik okamžiků před tím, než se z něj muž, který zavolal policii, pokusil vybrat peníze. Šlo o tříčlennou posádku stříbrné Alfy Romeo.
Kriminalistům se podařilo během jediného dne zjistit, že se trojlístek pohyboval na Strakonicku, Písecku i Táborsku. Vypátrali, že naposledy bylo auto v Plané nad Lužnicí. "Hned druhý den, proto zorganizovali akci, při níž celou posádku zadrželi v autě, když projížděla Táborem. Cizinci patří s největší pravděpodobností k mezinárodnímu gangu, který padělá platební karty a jsou vedeni v evropské evidenci zaměřené na zájmové osoby v oblasti skimmingu," upřesnila Uhlířová s tím, že jeden z nich byl už za tento trestný čin v minulosti odsouzen. Další úspěch zaznamenali kriminalisté při čtvrteční domovní prohlídce penzionu v Plané nad Lužnicí, kde tato trojice pobývala. V jejich apartmá objevili nástavec hrdla bankomatu pro vstup platební karty, lištu se skrytou kamerou a zdrojem a další padělatelské příslušenství. Ukázalo se, že podezřelí napadli i další bankomaty nejen na území Jihočeského kraje, ale také v kraji Jihomoravském, Plzeňském a v kraji Vysočina. "V Blatné však udělali chybu, když pravděpodobně v časové tísni nedokonale nainstalovali čtecí zařízení na zmíněný bankomat," podotkla policejní mluvčí. Všichni tři muži skončili ve vazbě s obviněním z trestného činu neoprávněné opatření, padělání a pozměnění platebního prostředku a výroba a držení padělatelského náčiní. Při prokázání viny jim hrozí až osmileté vězení

„Mistr převleků“ vykradl v Praze několik bank

Mistr převleků. Tak začali policisté přezdívat muži, který vyloupil čtyři pražské banky. Zprvu se zdálo, že jednotlivá přepadení nesouvisí. Nakonec kriminalisté prokázali, že pachatel pouze šikovně klame za pomocí různých převleků. Na jednom záznamu vypadá na třicet let, na dalším na šedesát. Poprvé o sobě dal vědět 21. června. Tehdy přišel do bankovního ústavu v Lidické ulici s balíčkem, o němž hovořil jako o výbušnině. Pokladní mu v obavách o svůj život dala peníze do připravené igelitky. Tehdy se maskoval červenou kšiltovkou a velkými dioptrickými brýlemi.
Druhé přepadení se odehrálo o jedenáct dní později v ulici Lazarské v Praze 2. "To proběhlo úplně stejným způsobem a pachatel si také odnesl finanční hotovost," připomněla mluvčí pražské policie Eva Kropáčová. Tentokrát však pachatel nechal doma šusťákovou bundu i čepici a oblékl špatně padnoucí tmavé sako a myslivecký klobouk. Nutno podotknout, že na záběrech z loupežného přepadení druhé banky vypadá o mnoho mladší, než na snímcích pořízených během prvního přepadení v ČSOB. Zprvu tak nebylo nasnadě předpokládat, že jde o stejného

pachatele. Třetí přepadení na Arbesově náměstí už zločinci nevyšlo. "Pokladní mu odmítla dát peníze a utekla do zadních prostor provozovny," podotkla mluvčí. Zpackaná akce ho neodradila a následující den se vrátil do banky v Lazarské, kde už jednou uspěl. "Nyní již však pokladní ukázal, že má střelnou zbraň a při přepadení byl mnohem agresivnější. Žena mu do igelitové tašky naskládala peníze a on, jako by se nic nedělo, odešel pryč," vylíčila Kropáčová.
Při posledních dvou přepadeních se pachatel rovněž maskoval kšiltovkou a brýlemi. Po "akci" použitý oděv pokaždé vyhodil nedaleko místa činu. Přestože se to z kamerových záznamů pocházejících z bank zdálo nepravděpodobné, kriminalisté věděli, že se jedná o stejného muže, který se snaží pouze policisty a okolí zmást.
Nakonec byl muž 26. července zadržen přímo ve svém domě ve Středočeském kraji. Při výslechu se ke všem čtyřem loupežím doznal a svého jednání velmi litoval. Údajně jej k němu dohnala špatná životní situace a dluhy.

Sérii bankovních přepadení měla na svědomí žena

Poprvé v lednu, podruhé na začátku července a hned o den později potřetí loupila třiačtyřicetiletá žena z Českých Budějovic v bankách a směnárně. Neváhala přitom hrozit zbraní. Jen několik minut po poslední akci ji policisté zatkli. Hrozí jí až deset let vězení.
První případ se stal v lednu letošního roku v Českých Budějovicích. "Žena pod výhrůžkou použití zbraně získala od pracovnice banky finanční hotovost v řádech několika desítek tisíc korun," sdělil jihočeský policejní mluvčí Milan Bajcura. Peníze schovala do tašky a zmizela. Začátkem července žena udeřila podruhé, tentokrát si vybrala menší pobočku banky na Českobudějovicku, kde stejným způsobem, se zbraní v ruce, požadovala peníze. Pokladní odmítla, což lupičku natolik zaskočilo, že odešla s prázdnou. "Už den nato se však vrátila opět do krajského města, kde ve směnárně znovu se zbraní položila na pult tašku a požadovala vydání hotovosti," upozornil Bajcura. Toto přepadení však bylo na dlouhou dobu poslední, ke kterému se odhodlala.
Lupičky si ve směnárně všiml svědek, který okamžitě zavolal policisty. Ti ji brzy chytili. Vyšetřováním posledního případu pak kriminalisté objasnili také předchozí dva. Za loupeže jí teď hrozí dva roky až deset let odnětí svobody.

Klient se omylem dostal do interní databáze Komerční banky.

Jiří Dlabaja má účet u Komerční banky, v úterý dopoledne se mu ale podařilo při přihlašování do svého internetového bankovnictví dostat nejen ke svým, ale i k interním datům banky a k citlivým informacím o jiných klientech. "Omylem jsem se naboural do interních databází Komerční banky. Jména, rodná čísla, adresy bydliště, e-maily, jak se klienti chovali," vypočítává na svém facebookovém profilu bývalý reportér televize Nova a nynější mluvčí AŽD Praha Jiří Dlabaja. Podle údajů na stránce se dostal až k 47 tisícům kontaktů, které mohl i sám editovat a přepisovat. Že se tímto problémem v Komerční bance zabývají, potvrdila i její mluvčí Monika Klucová.
"Komerční banka v úterý ráno identifikovala technickou chybu informačního systému Penzijní společnosti Komerční banky. Touto situací se velmi vážně zabýváme a neprodleně jsme zahájili veškerá nezbytná opatření k jejímu vyřešení," řekla Klucová pro IHNED.cz s dodatkem, že může ubezpečit všechny klienty, že nedošlo k žádnému ohrožení bezpečnosti či k úniku informací o bankovních účtech klientů. Za chybu může podle vyjádření banky dodavatel systému. "Chyba v informačním systému, jehož vývoj pro Penzijní společnost KB zabezpečuje externí dodavatel, jímž je firma Softip, umožnila neoprávněný přístup do kontaktní databáze," uvedl Pavel Jirák, předseda představenstva Penzijní společnosti KB.
"V žádném případě nedošlo k úniku informací o již uzavřených smlouvách o penzijním spoření nebo o stavu prostředků na účtech klientů," dodal Jirák. A Klucová doplnila, že se "v žádném případě nejedná o chybu internetového bankovnictví KB, je to chyba v jednom modulu webové aplikace Penzijní společnosti KB." Mluvčí PF KB uvedla, že společnost bude své klienty kvůli tomuto problému kontaktovat.

Úvěrový podvodníci nechávali bezdomovce zakládat bankovní účty

Pražští kriminalisté odhalili trojici úvěrových podvodníků. Muži původem ze Slovenska si pomocí sociálně slabých otevírali účty v bankách. Na ty si potom nechali posílat peníze z půjček, které získali za pomoci falešných dokladů. V devatenácti případech tak způsobili celkovou škodu 1,5 milionu. Trojice Slováků trvale žijící v Česku si vybírala zejména bezdomovce, ale i mladé lidi po škole, kteří neměli práci. Ty pak připravila na jednání v bance. Bezdomovce umyla, oblékla, vybavila telefonem. Oblečení i telefony ale po založení konta nastrčeným lidem zase sebrala.

Za založení konta a pozdější zaslání kreditních karet ke kontům slibovali podvodníci odměnu v řádu tisícikorun, nakonec ale vypláceli jednu až tři stokoruny, jen výjimečně i o něco více. Na takto získané účty si potom nechávali posílat od finančních institucí půjčky. Ty už sjednávali sami. Využívali k tomu nejrůznějších padělaných dokladů. Peníze poté používali pro vlastní potřebu. "Použili je zejména na nákup značkového oblečení," řekl vedoucí šestého oddělení policie Praha 2 Roman Hájek. Kriminalistům nebyli pachatelé neznámí. "Organizátor byl několikrát stíhaný za loupežné přepadení a vícekrát se dopustil majetkových trestných činů. Ty má na svědomí také druhý z mužů. Poslední z trojice zatím nebyl trestán," vysvětlil Hájek. Všichni jsou obvinění z úvěrového podvodu, hrozí jim dva až osm let vězení.

O půjčkách v bance rozhodují i facebookové profily

Vaši facebookoví přátelé mohou podle serveru CNN mít velmi významný vliv na vaše osobní finance. Ne snad tím, že by od vás na chatu vylákávali údaje k platební kartě. Spíše vás může virtuální přátelství s "nesprávnými lidmi" připravit o finance, které jste si teprve chtěli půjčit.

Tradiční poskytovatelé půjček se při vyhodnocování rizik většinou řídí údaji o úvěrové historii konkrétních potenciálních věřitelů. To má ale jeden háček – jsou jím miliony lidí, kteří dosud žádnou půjčku registrovanou nemají, a tak jejich solventnost nelze z těchto údajů zjistit. Pro tyto příležitosti nastupují nové nástroje, které se snaží vyčíst podobné údaje z profilů na sociálních sítích. A z nich odvodit konkrétní schopnost dostát závazkům. Například finančníci z úvěrové společnosti Lenddo se soustředí na to, zda na Facebooku mezi svými přáteli nemáte někoho, kdo jim nesplácí podle plánu. Pokud ano, budete mít problém se sjednáním půjčky i vy. A pokud si s oním "neplatičem" často píšete nebo vzájemně "lajkujete" statusy, vaše startovní pozice v očích poskytovatele půjčky bude o to horší. Podle ředitele a zakladatele Lenddo Jeffa Stewarta vychází jejich strategie z jednoduchého předpokladu. "Lidé moc dobře vědí, kdo je v jejich okolí důvěryhodný a solidní. A my to jen nyní díky výpočetní technice můžeme jednoduše měřit," osvětluje pointu Stewart.

Údaje ze sociálních sítí používá také německá společnost Kreditech, která má zastoupení i v Praze. Jde na to ale trochu jinak. Tvrdí, že každého žadatele proklepnou z až 8 tisíců datových stop, které jsou k dispozici. Kromě údajů o účtech na Facebooku, eBay nebo Amazonu také analyzuje, jakým způsobem vyplňují žadatelé o půjčku jejich on-line formulář. Když například stráví zájemce hodně času čtením podmínek, jeho důvěryhodnost stoupne. Tyto nástroje a jejich poskytovatelé zatím cílí pouze na minoritní skupiny potenciálních vypůjčovatelů na trhu. Lenddo, které má na čtvrt milionu klientů, například operuje pouze na Filipínách, v Kolumbii a v Mexiku. Každopádně jsou ale podobné technologie podle CNN na cestě k tomu, aby se staly analytickým mainstreamem. Svědčí o tom strategie Kreditechu, který svou technologii dodává on-line poskytovatelům v Rusku či Česku.

Září

Scotland Yard zabránil kybernetické bankovní loupeži

Britská policie zatkla 12 mužů, kteří se podle ní chystali ukrást peníze z pobočky jednoho z největších finančních ústavů světa, španělské banky Santander, a to ovládnutím jejího počítače. Uvedl to server britské zpravodajské stanice BBC. Policisté našli zařízení, které podezřelí tajně připojili k počítači banky Santander v jihovýchodním Londýně a pomocí kterého mohli stahovat veškerá data o bankovních operacích.
„Zařízení propašoval do banky falešný technik údržby. Do celé akce nebyl zapojen žádný z našich zaměstnanců," uvedl mluvčí Santanderu. Údržbu poboček podle něj zajišťuje najatá agentura. Zatčení muži ve věku 23 až 50 let by podle policie připravili banku o mnoho miliónů liber. „K žádným penězům se ale nedostali," zdůraznil mluvčí banky.

Úvěrový podvod mezi sousedy rozkryli policisté na Brněnsku
Případ úvěrového podvodu, ve kterém figurovaly dvě bývalé kamarádky, vyřešili policisté v Dolních Kounicích na Brněnsku. Padesátiletá žena tam zneužila důvěry své sousedky, aby se dostala k jejím dokumentům. Na její jméno si pak vzala stotisícovou půjčku. Ženy se dobře znaly a jako sousedky si navzájem vyměnily i klíče od domu. "Mladší žena, když nebyla kamarádka doma, prohledala její obydlí a vyhledala si potřebné údaje a dokumenty k získání skoro stotisícového úvěru. Ten jí úvěrová společnost poskytla a podvodnice pak pomocí platební karty, kterou k půjčce získala, peníze vyčerpala," popsal brněnský policejní mluvčí Bohumil Malášek.
Díky neomezenému přístupu do sousedčina domu dokázala podvodnice také průběžně likvidovat poštu od úvěrové společnosti, která nic netušící ženě chodila. "Případ vyšel najevo až ve chvíli, kdy se u domu zaskočené sousedky objevil exekutor. Než se celý případ podařilo vyšetřit, žena přišla o více než deset tisíc korun, které jí byly v rámci exekuce na celý dům strženy z penze," řekl Malášek. Sousedka je teď stíhaná pro podvod, neoprávněné držení platební karty a porušování tajemství dopravovaných zpráv.

Říjen

Další případ viru cílí na české internetové bankovnictví
V jedné z předchozích situačních zpráv jsme informovali o viru Eurograbber, který byl jedním z prvních zaznamenaných případů úspěšného prolomení dvoufaktorové autorizace pro přístup do internetového bankovnictví (zasílání autorizačních SMS na mobilní telefon). Podle očekávání následovali jeho příkladu další tvůrci malware, takže na podzim vydala Česká bankovní asociace nové varování před phishingovými útoky, které se pokouší ovládnout jak počítač, tak mobilní telefon uživatele. Scénář je obdobný jako v minulosti. Klient je virem nevědomky přesměrován do podvrženého systému internetového bankovnictví, kde je mu nabídnuta instalace nového bezpečnostního balíčku na mobilní telefon. Po technické stránce je nový virus opět o něco sofistikovanější. Systémy bank ani v tomto případě napadeny nebyly, virus opět zneužívá důvěry klientů. Vzhledem ke stále nově se objevujícím hrozbám v této oblasti, je proto nutné nespoléhat pouze na antivirové programy (nějakou dobu trvá, než jsou aktualizovány na nové typy malware), ale dodržovat známá opatření pro ochranu proti tomuto typu phishingu tj. pro mobilní internetové bankovnictví používat pouze autorizované aplikace z oficiálních marketů, dávat pozor na podvržené stránky, které vypadají téměř identicky jako aplikace bank, neinstalovat neznámý software – pokud si nejsme zcela jistí, je možné kontaktovat banku a jeho pravost si ověřit. Tipy pro bezpečnost mobilních zařízení přinášíme také v této Situační zprávě, v kapitole věnované kybernetické bezpečnosti. Mimořádné opatrnosti je třeba dbát při otevírání emailových zpráv – právě skrz ně probíhají phishingové útoky nejčastěji. Klient by měl také pravidelně kontrolovat svůj bankovní účet a zůstatek na něm – čím dříve je problém odhalen, tím menší škoda může být napáchána. Více viz tisková zpráva České bankovní asociace zde:
http://www.csas.cz/static_internet/cs/Komunikace/Tiskove_centrum/Tiskove_zpravy_a_aktuality/Prilohy/tz_cba_20131004_hacker_utok.pdf

Policie dopadla lupiče, který vykradl čtyři banky v Třebíči a v Praze

Po více než čtyřech letech se policii podařilo dopadnout lupiče, který v únoru roku 2009 přepadl s pistolí v ruce banku v Třebíči. Z ní si i pod záběrem bezpečnostních kamer odnesl statisíce. Nyní se ukázalo, že stejný lupič vykradl i třikrát banku v Praze. Z bank si celkem odnesl přes 1,3 milionu korun.

Pobočka ČSOB na Karlově náměstí v Třebíči byla prvním peněžním ústavem, který si vyhlédl a 25. února 2009 kolem půl třetí odpoledne do ní maskovaný vešel. Pak vytáhl pistoli. "Zbraň namířil na zaměstnance banky a ostrahu a pod pohrůžkou použití zbraně si vynutil vydání finanční hotovosti ve výši 653 tisíc korun," připomněla policejní mluvčí Dana Čírtková. Pak se po něm na dlouhou dobu jakoby slehla zem. Kriminalisté nemohli jeho maskování, zachycené na kamerovém záznamu, odhalit. Až v říjnu se kriminalistům podařilo muže vypátrat. Loupež měl na svědomí sedmadvacetiletý muž s trvalým pobytem na Třebíčsku, který nyní pobýval v Praze. Po stopách tohoto zločince pátrali nejen kriminalisté z Vysočiny, ale také jejich pražští kolegové. Ukázalo se, že muž má na svědomí kromě přepadení třebíčské banky ještě tři další loupeže v pražských bankách. Při všech si počínal podobně a také hrozil pistolí.

K prvnímu pražskému přepadení došlo 27. listopadu 2009, kdy přepadl pobočku Raiffeisen bank v Praze 9. I tehdy měl u sebe zbraň a na obsluze pokladny si vynutil vydání 320 tisíc korun. K další loupeži se odhodlal až skoro za rok, 27. září 2010, kdy kolem deváté hodiny ráno přepadl pobočku Komerční banky, rovněž v Praze 9. I tam pokladní ve strachu o svůj život lupiči vydala na pokladní přepážku 364 tisíc. Ke svému poslednímu přepadení si lupič vybral 7. srpen letošního roku. Krátce po poledni vešel maskovaný do pobočky UniCredit Bank v Praze 7. I tam použil k výhrůžkám zbraň. Pokladní lupiči vydala 39 tisíc.

Po dopadení se lupič policistům přiznal. Vyšetřovatelům uvedl, že měl dluhy, a proto potřeboval peníze, které si rozhodl opatřit bankovními loupežemi. Minulý pátek ho kriminalisté obvinili z loupeže, ještě podle trestního zákona účinného do 31. prosince 2009 a také ze zvlášť závažného zločinu loupeže podle v současné době platného trestního zákoníku. "Obviněný muž byl eskortován do vazební věznice v Brně," dodala policejní mluvčí Čírtková. Za čtyři spáchaná loupežná přepadení peněžních ústavů, která spáchal na Vysočině a v Praze mu hrozí pět až dvanáct let za mřížemi.

Obžalovaný z „loupeže století“ u soudu popírá svou vinu

Někdejší dispečer bezpečnostní agentury G4S Antonín Saleta u soudu popřel, že by pomáhal neznámým pachatelům s takzvanou loupeží století. Soudu přesto nedokázal vysvětlit, jak po loupeži náhle zbohatnul.

Loupež se stala v září 2002 na pražské Evropské třídě. Lupiči pohrozili posádce pancéřového vozu atrapou výbušniny a samopalem a přinutili ji, aby auto otevřela a přemístila se do jeho zadní části. Pak s vozem odjeli k nádrži Jiviny, kde z něj sebrali peníze. Obžaloba tvrdí, že Saleta zařídil, aby v přepadeném voze G4S seděl řidič, který lupičům nekladl odpor. Muži převlečení za policisty z auta vzali 154 milionů korun, jež se dodnes nenašly. "Obžalovaný jako pracovník operačního střediska firmy G4S přepadení plánoval a poskytl zkušenosti s ovládáním vozidla, zvláště s otevíráním dveří," uvedl při čtení obžaloby státní zástupce Tomáš Saňa. Lupičům se totiž podle svědků podařilo otevřít zadní dveře vozu hned napoprvé, což vyžadovalo stisknutí přesné kombinace tlačítek na palubní desce.

"Čin jsem nespáchal," prohlásil stručně třiačtyřicetiletý Saleta, který následující dvě hodiny čelil otázkám ze strany soudního senátu, žalobce i svého advokáta. Odmítl, že by směny řidičů vyměnil právě on. Dotazy předsedy senátu Stanislava Králíka na své "zázračné zbohatnutí" po loupeži odbýval s tím, že o peníze nikdy neměl nouzi, a když přece jen nějaké potřeboval, půjčil si je. Přesto však nedokázal jasně vysvětlit, kde s měsíčním platem zhruba 30 000 korun náhle vzal peníze na pilotní kurz, koupi bytu a cesty do Karibiku. Obžaloba z loupeže století původně vinila čtyři lidi: vedle Salety také Františka Hajna a členy Berdychova gangu Tomáše Půtu a Maroše Šuleje. Šuleje, Půtu i Hajna, který se procesu dlouho vyhýbal pobytem v Dominikánské republice,

však už soudy pravomocně zprostily viny kvůli nedostatku důkazů. Po Saletově dopadení ve Venezuele se protáhlo jeho vydávací řízení, a proto soud jeho čin vyloučil k samostatnému projednání. Policie muže eskortovala do Prahy v srpnu 2013.

Podvodník sliboval vyřízení úvěrů, u banky přitom dávno nepracoval
Policisté z Českobudějovicka stíhají kvůli podvodu osmatřicetiletého bývalého pracovníka banky. Lidem nasliboval zařízení úvěrů, k čemuž však po propuštění už neměl žádnou pravomoc. Za vyřízení přitom inkasoval pětitisícové poplatky. Během svého působení v bance získal mnoho zkušeností, a to především jak jednat s klienty a nabízet jim nejrůznější produkty.
"Těchto schopností využil pro spáchání několika podvodů. Přesto, že už u bankovní společnosti zaměstnán nebyl, vystupoval stále jako finanční makléř zastupující různé společnosti," vylíčila českobudějovická policejní mluvčí Štěpánka Uhlířová. Podvodník takto ošálil devět lidí, kteří na základě sepsaných žádostí o úvěr, které jim muž nemohl vyřídit, poslali vysokou zálohu za zprostředkování. "Účtoval si poplatek za vyřízení této žádosti ve výši 5 250 korun. Celkem devět osob tuto částku zaslalo bankovním převodem na dohodnutý účet," upřesnila mluvčí. Téměř padesát tisíc korun, o které "klienty" obral, pak pachatel použil pro vlastní potřebu. "Specialisté na hospodářskou trestnou činnost muže obvinili z trestného činu podvodu. Je stíhán na svobodě," doplnila Uhlířová.

Listopad

ČNB bude přísněji regulovat banky, jejichž krach by ohrozil ČR

Centrální banka rozhodla, že čtyři české banky jsou tak velké, že by jejich případný pád mohl dostat do potíží český finanční systém a s tím i celou ekonomiku. Podle oslovených ekonomů se jedná o ČSOB, Českou spořitelnu, Komerční banku a UniCredit Bank. Čtyři vybrané banky budou muset mít kapitálové rezervy o jedno až tři procenta vyšší než ostatní. Aby byla pravděpodobnost jejich krachu či dalších potíží co nejmenší. Pro střadatele, kteří si ukládají do systémových bank peníze, se nic nezmění. Banky zřejmě nezvýší z důvodu nové regulace ani poplatky za své služby, i když povinnost hlásit ČNB další údaje pro ně bude znamenat vyšší náklady.

Dvojice úvěrových podvodníků připravila banku o 33 milionů korun
Úřednice banky a externí zaměstnanec peněžního ústavu padělali od roku 2007 celkem 112 žádostí o úvěr. Banku tím připravili o více než třicet milionů korun. Muže nyní detektivové obvinili z trestného činu podvodu, ženě stejné obvinění sdělili už v lednu.
"Jednačtyřicetiletý muž pracoval externě pro bankovní ústav a s o pět let starší zaměstnankyní pak uzavírali smlouvy s neexistujícími osobami. Úřednice následně proplácela schválené žádosti o úvěr na bankovní účet obviněného," uvedla policejní mluvčí Jana Rösslerová. V dubnu roku 2010 o podezřelých transakcích informovali zástupci banky policii. Úřednici v lednu tohoto roku sdělili kriminalisté obvinění z trestného činu podvodu. Podezřelého zadrželi 30. října v Jesenici u Prahy. Muži vzhledem k výši způsobené škody hrozí až desetileté vězení. Nakradené peníze si dovedl náležitě užívat. Navštěvoval například luxusní restaurace, koupil si luxusní vůz i nemovitost za šest milionů korun.

Americké banky od roku 2015 skončí s rizikovým obchodováním na vlastní účet
Banky ve Spojených státech budou moci na finančních trzích obchodovat jen pro své klienty, na vlastní účet to budou moci dělat jen na svou ochranu před tržními riziky anebo při úpisech cenných papírů. Tak zní konečná verze takzvaného Volckerova pravidla, na němž se dnes shodlo pět amerických regulačních úřadů. Zákaz obchodů na vlastní účet, založený na zákoně o reformě finančního sektoru z roku 2010, začne pro největší banky platit až od roku 2015. Zákon, který reagoval na hlubokou finanční krizi, nastínil obecné pravidlo nazvané podle někdejšího šéfa centrální banky (Fed) Paula Volckera. Ten prosazoval, aby banky měly zakázáno ohrožovat

peníze vkladatelů rizikovými obchody na vlastní účet. Banky může regulace připravit o miliardy dolarů na ziscích, bankovní sektor by ale měl být podle představ regulačních orgánů díky tomu bezpečnější a odolnější vůči finančním krizím.
Opatření vstupují v platnost v červenci 2015, což je o rok později, než se předpokládalo. Regulační úřady opakovaně překračovaly v dokončení Volckerova pravidla stanovené termíny a regulace se mezitím rozrostla na téměř 900 stránek textu.

Prosinec

Pachatel, instalující do bankomatů skimmovací zařízení, byl chycen v Karlovarském kraji
Policisté v Karlovarském kraji překazili pokus o okradení klientů bank prostřednictvím údajů získaných z jejich platebních karet. Skupina cizinců umístila na bankomaty v regionu čtecí zařízení pro zkopírování identifikačních a přístupových údajů ke kartě. Policisté jednoho z pachatelů zadrželi. Neupřesněný počet takzvaných skimmovacích zařízení pachatel či pachatelé nainstalovali na vybrané bankomaty 6. prosince v brzkých ranních hodinách.
"Po zjištění, že na bankomatech se nachází skimmovací zařízení, byla provedena rozsáhlá policejní akce a v nočních hodinách byl zadržen sedmadvacetiletý cizinec, který se právě snažil sundat skimmovací zařízení z bankovních terminálů," popsal policejní mluvčí Pavel Valenta.
Zadrženého cizince policisté obvinili ze zločinu neoprávněného opatření, padělání a pozměnění platebního prostředku. V případě prokázání viny mu hrozí až osm let ve vězení. "Pokud by se prokázalo, že byl součástí organizované skupiny, hrozí pachateli trest odnětí svobody až na dvanáct let," uvedl Valenta. Soudce Okresního soudu v Chebu akceptoval návrh státního zástupce a obviněného poslal do vazby.

Další pachatelé skimmingu zadrženi v Havlíčkově Brodě
Policisté na Vysočině zadrželi dva cizince kvůli takzvanému skimmingu. Muži jsou podezřelí, že na několik bankomatů v Havlíčkově Brodě namontovali zařízení, které mělo pachatelům umožnit kopírovat údaje z magnetického proužku platebních karet.
Policie zadržela dva cizince ve věku 27 a 44 let, kteří pocházejí z jedné ze zemí na Balkáně. "Kriminalisté zadrželi oba cizince přímo při činu, když se zařízením bankomatu manipulovali," uvedla krajská policejní mluvčí Dana Čírtková. Muži jsou ve vazební věznici v Hradci Králové.
"Byli obviněni z trestného činu neoprávněného opatření, padělání a pozměnění platebního prostředku. V případě odsouzení mohou dostat trest odnětí svobody až na osm let," dodala mluvčí. Nalezené skimmovací zařízení bude nyní podrobeno odbornému znaleckému zkoumání v pražském kriminalistickém ústavu. Skenovací zařízení na bankomatu zajistili v stejném týdnu také policisté v Chrudimi na Pardubicku. Podle vyjádření tamní krajské policejní mluvčí Jitky Vavřinové šlo o kameru a čtečku magnetických pásků na kreditních kartách. Podle policie mohou případy souviset.

Německá policie provedla razii v Commerzbank kvůli daňovým podvodům

Němečtí vyšetřovatelé od úterního dopoledne zasahují ve zhruba 40 pobočkách finančního ústavu Commerzbank, který je druhou největší bankou v Německu. Důvodem je podezření z napomáhání k daňovým podvodům údajně za stovky milionů eur. Oznámilo to bochumské státní zastupitelství, podle něhož není podezřelá samotná banka, ale pracovníci zahraniční pojišťovny, která s ní spolupracuje. Podle serveru hospodářského listu Handelsblatt se celoněmecké razie účastní na 270 vyšetřovatelů, kteří zasahují nejen ve filiálkách banky, ale i v její centrále ve Frankfurtu nad Mohanem. "Vyšetřování nesměřuje proti bance, ale proti jednotlivým spolupracovníkům jiného poskytovatele finančních služeb," potvrdil agentuře DPA mluvčí Commerzbank. Podle informací Handelsblattu úřady očekávají, že naleznou důkazy o daňových podvodech za několik stovek milionů eur. Konkrétně má jít o podvody se životními pojistkami v ústavu, který patří nejmenovanému italskému pojišťovacímu koncernu. Vyšetřování

podle listu spustilo zářijové odhalení nesrovnalostí u jednoho daňového přiznání v nejlidnatější německé spolkové zemi Severním Porýní-Vestfálsku. Server deníku Frankfurter Allgemeine Zeitung uvedl, že pracovníci pojišťovny jsou podezřelí, že s ukrýváním peněz před finančními úřady napomáhali už od roku 2006. Před rokem podnikla německá policie podobnou razii v pobočkách a ve vedení Deutsche Bank. Prokuratura poté uvalila vazbu na pět zaměstnanců největší banky v zemi. Obviněni byli z praní špinavých peněz a z krácení daní při obchodování s emisními povolenkami.

EU schválila pilíře bankovní unie. Jde o největší změnu od zavedení eura

Dohodou o rozhodovacím mechanismu se zkompletovaly přípravy na evropskou bankovní unii a její záchranný mechanismus. Aktuální kompromis navazuje na předchozí dohody ministrů eurozóny o záchranném bankovním fondu a dohledových pravomocích Evropské centrální banky. O osudu velkých bank v zemích eurozóny už nebudou rozhodovat jednotlivé země samostatně, ale společná instituce. To je největší změna Evropské unie od dob zavedení eura. Po společném dozoru nad bankami jde o další krok při vytváření bankovní unie, která má zabránit v případě krize rozpadu eurozóny. Politická shoda ale vede k tomu, že o osudu bank v problémech – zda je zavřít, rozprodat či jim pomoci – bude někdy rozhodovat více než sto lidí. Výsledkem snahy uklidnit nejrůznější výhrady unijních zemí je totiž poměrně složitý mechanismus, v němž budou moci mít své slovo státy i Evropská komise. Prvním pilířem je již dříve schválená funkce Evropské centrální banky (ECB) coby supervizora. Druhý pilíř představuje podle BBC takzvaný jednotný záchranný mechanismus (SRM - Single Resolution Mechanism) a třetím je samotný společný záchranný fond.

České banky obstály v zátěžových testech ČNB a jsou odolně vůči rizikům

Tuzemské banky jako celek jsou podle aktuálních výsledků zátěžových testů, které provedla Česká národní banka, dál odolné vůči případnému nepříznivému vývoji. Kapitálová přiměřenost celého sektoru by zůstala výrazně nad požadovaným osmiprocentním minimem i ve scénáři, který pro následující tři roky předpokládá pokračování recese. O výsledcích informovala ČNB. Zároveň ale centrální banka upozornila, že v základním i alternativním scénáři by některé banky musely doplnit kapitál. Výsledky jsou tak podobné předchozím testům, které ČNB zveřejnila letos v červnu. Ke konci září kapitálová přiměřenost bank přesahovala 17 procent. Centrální banka prohlásila, že ve srovnání s výsledky zátěžových testů z června vykazuje bankovní sektor pro základní scénář vyšší míru odolností.

Zdroje pro tuto kapitolu: policie.cz, cyprus-mail.com, ihned.cz, idnes.cz, bakerstreet.wikia.com, novinky.cz, csas.cz, cnb.cz, newmoney.gov, europeum.org, bvv.cz, banktech.com, sxc.hu, cnn.com.

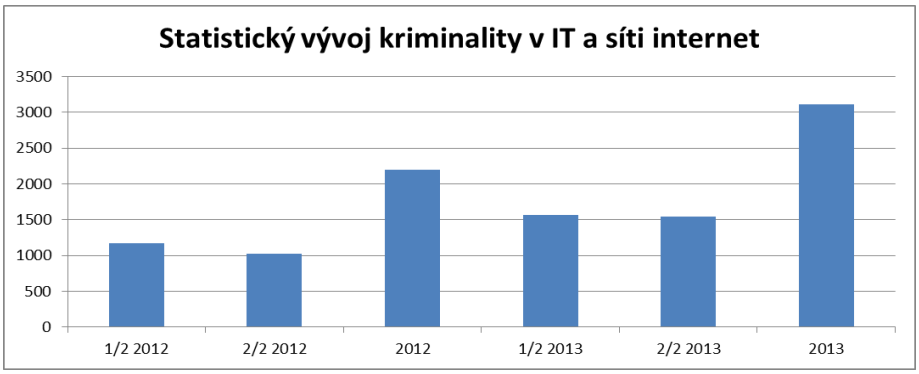
INFORMAČNÍ TECHNOLOGIE A KYBERNETICKÁ BEZPEČNOST

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.

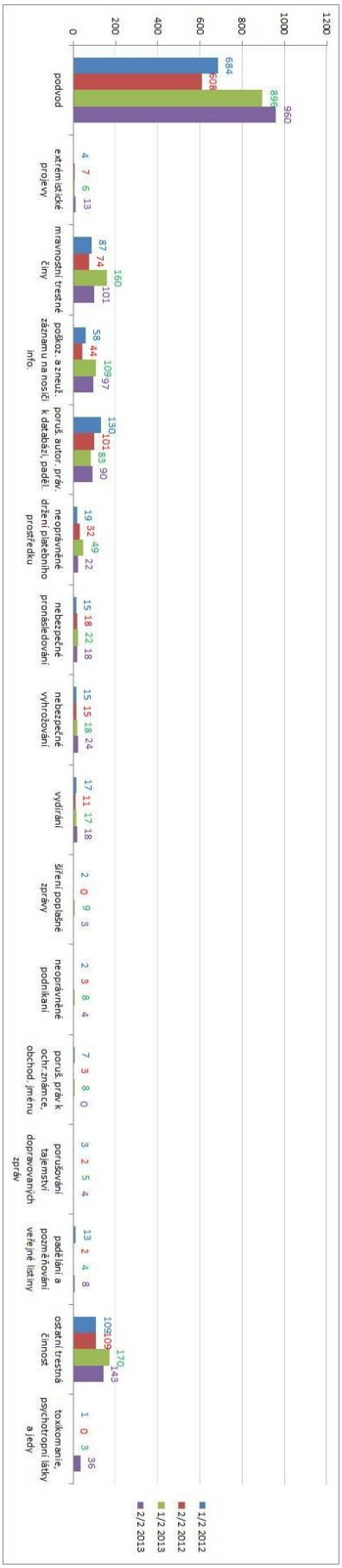
Informační kriminalitou rozumíme takovou trestnou činnost, která je **páchána v prostředí informačních technologií**, kdy předmětem útoku je buď samotná oblast informačních technologií, případně je tato trestná činnost prováděna za výrazného využití informačních technologií.

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).

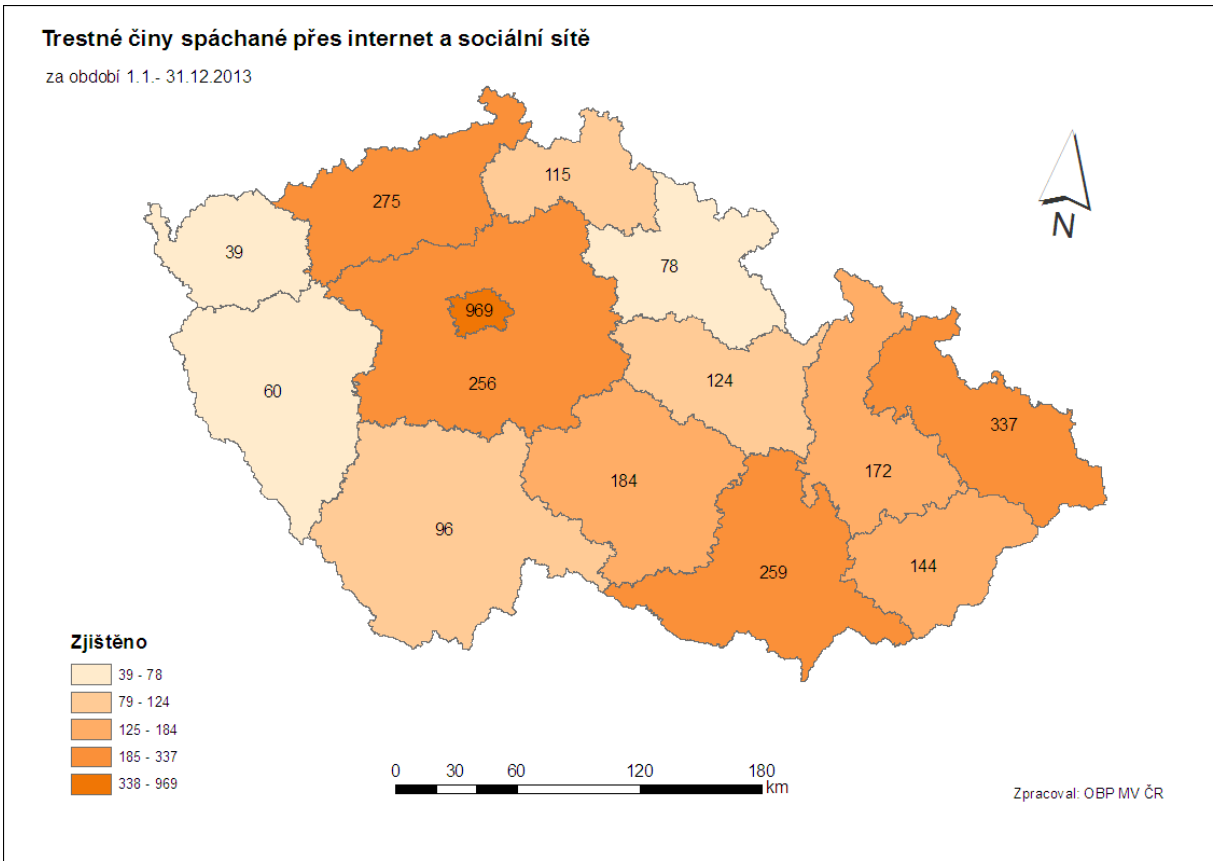


Nejčastější projevy tzv. informační kriminality, která je, jak je patrné z výše uvedeného grafu, na neustálém vzestupu, byly v minulosti zejména charakteru porušení autorských práv, výhrůžek, vydírání atd. **Aktuální dominance je nicméně v oblasti podvodných jednání**, kde je zaznamenáván neustálý nárůst a kdy tyto jednání jsou současně majoritního charakteru vůči ostatní páchané trestné činnosti v prostředí IT a sítě internet, jak je graficky znázorněno na následující straně.

Na neustálém vzestupu jsou útoky formou tzv. phishingu, iniciované plošnou spamovou distribucí. Nově se jedná o zaznamenávání přístupových kódů, sloužících aktuálně i k podvodnému přístupu na bankovní účty cestou elektronického bankovnictví, z nichž jsou pak neoprávněně odčerpávány finanční prostředky.


1200
1000
800
600
400
200
0
684
608
896
960
podvod
4 7 6 13
extrémistické projevy
87 74 160 101
hromadné trestné činy
58 44 109 97
poškoz. a zneužití záznamu na nosiči info.
130 101 83 90
poruš. autor. práv, držení padělk. databází
19 32 49 22
neoprávněné držení platebního prostředku
15 18 22 18
nebezpečné pronásledování
15 15 18 24
nebezpečné vyhrožování
17 11 17 18
vydírání
2 0 9 3
šíření poplašné zprávy
2 3 8 4
neoprávněné podnikání
7 3 8 0
poruš. práv k ochr.známce, obchod.jménu
3 2 5 4
porušování tajemství dopravovaných zpráv
13 2 4 8
padělání a pozměňování veřejné listiny
109 109 170 143
ostatní trestná činnost
1 0 3 36
toxikomanie, psychotropní látky a jedy
1/2 2012
2/2 2012
1/2 2013
2/2 2013

Celkem bylo v uplynulém roce 2013 prostřednictvím sítě internet **spácháno 3 108 trestných činů**. **Z toho celkem 1 740 tvořily různé formy podvodů**. Z dalších trestných činů byly výrazněji zastoupeny také neoprávněný přístup k počítačovému systému či nosiči informací (196 případů), výroba a nakládání s dětskou pornografií (174 případů) a porušení autorského práva a souvisejících práv (173 případů). Další druhy trestných činů následují ve své četnosti se značným odstupem, pro zajímavost lze uvést, že šíření poplašné zprávy přes internet policie vyšetřovala ve 12 případech. Geografické rozložení incidence informační kriminality v rámci ČR lze vidět na následující mapě.



Jak je patrné z následující tabulky, **součet výše škod všech skutků spáchaných prostřednictvím internetu** v uplynulém roce dosahuje astronomické výše **přes čtvrt miliardy korun**. Je přitom pravděpodobné, že skutečný objem bude výrazně vyšší, neboť v případě informační kriminality je policii nahlášena jen část případů. Policii se přitom podaří **objasnit zhruba 43% registrovaných skutků**.

trestné činy spáchané přes internet a sociální sítě za období leden až prosinec 2013

registrované skutky	3 108
počet skutků, u nichž byl zjištěn pachatel	1 327
škoda	238 344 400 Kč

Zdroj: PČR

Dané technologie využívají rovněž předem vytvořeného prostředí ve formě tzv. botnetových sítí, tj. primárně útokem vytvořených cílových stanic, určených přes rozličné architektury sítí k páchání dalších kriminálních aktivit. V letošním roce je mimo jiné na místě poukázat na dvě masivní vlny phishingových útoků na bankovní instituce. Ty souběžně útočily jak na prostředí uživatelů osobních počítačů, tak i na prostředí mobilních komunikačních zařízení, přes něž jsou prováděny nejčastěji autorizace přístupů do účtů. Na našem území nebyl prozatím

zaznamenán častý výskyt samotných organizátorů takovéhoto jednání, nicméně často se v naší jurisdikci **vyskytují tzv. bílí koně („e-mules“)**, kteří mají za úkol převzít na svůj účet neoprávněně odčerpané prostředky z účtu poškozeného a ty jiným platebním kanálem poslat dále tak, jak jsou instruováni.

Vhodné je rovněž poukázat, že oproti minulosti policie zaznamenala na našem území umisťování vzdáleně spravovaných komunikačních prvků pachatelů působících v kybernetickém prostředí. V hodnoceném období jsou také neustále zaznamenávány **snahy o umístění phishingových stránek kybernetických útoků pachatelů z jiných zemí**, odkud pocházejí také oběti těchto útoků. Česká republika pak těmto hackerům slouží pouze jako „technické zázemí“.

Policie také detekovala výskyty krádeží identit, které jsou zneužívány ať už ke kompromitaci faktických subjektů, anebo jako legendy pro páchání zejména podvodných jednání. Nově u podvodných jednání začal být zaznamenáván **nárůst převodu finančních prostředků do virtuálních internetových měn**. Tyto měny jsou rovněž často využívány i k platbám za ilegální zboží, a to nejčastěji v rámci obchodů sjednávaných v síti TOR.

Pachatelé informační kriminality velmi rychle reagují na technologický vývoj a využívají jej ve svůj prospěch. Jak roste poměr počtu mobilních zařízení a význam zpracovávaných dat v těchto mobilních zařízeních, tak narůstá i šíření mobilního malware a množí se útoky na tato zařízení. Profesionalizace pachatelů informační kriminality bude mít do budoucna stále větší míru propracovanosti s jasnější dělbou jednotlivých rolí. Tento trend je již z hlediska českých kriminalistů jasně pozorovatelný. Větší bude i **zapojení tzv. botnetových sítí**, které mají za úkol anonymizovat aktivitu původce nelegálního jednání a současně zvyšovat masivnost či technologickou koordinaci útoku.

Uplynulý rok je možné jednoznačně definovat jako zlomový ve využívání tzv. cloudových řešení (ta označují vzdálená úložiště a správu dat). Do budoucna tak lze předpokládat větší míru útoků na takto centralizovaná data, kdy v případě prolomení ochrany bude docházet k masivnějším únikům informací, než tomu bylo doposud. Nové technologie nabízejí (a budou nabízet) stále větší možnosti pachatelům veškeré trestné činnosti zastírat vzájemnou komunikaci či výměnu dat s využitím nových typů IT služeb.

V delším výhledu pak je zcela zjevné, že s ohledem na optimalizaci nákladů, dostupnost přístupu a výměnu a archivaci veškeré komunikace, bude většina nepřímé komunikace digitalizována. Bude neustále růst objem a rozsah veškerých takto zaznamenávaných lidských aktivit. To se týká nejen běžného druhu obsahu, ale stejně tak i citlivých, osobních či jinak chráněných dat. V tomto ohledu bude exponenciálně růst míra důležitosti ochrany a nutnosti adekvátního opatření při narušování této ochrany, která ve většině případů bude mít kriminální charakter.

Případy informační kriminality z uplynulého roku

Pro ilustraci výše uvedených statistik můžeme uvést několik případů, se kterými se v roce 2013 čeští kriminalisté setkali.

Jak již bylo řečeno, z hlediska počtu jsou v současnosti v ČR dominantním trestným činem v prostředí informačních technologií různé druhy podvodů. Příkladem pachatelů takového jednání mohou být dva mladí lidé z Karlovarska, kteří provozovali **falešný internetový obchod**. Jednadvacetiletý mladík přes něj nabízel elektroniku (mobilní telefony, notebooky),

za které požadoval platbu předem, či alespoň zálohu na účty, které za tímto účelem založila jeho o rok mladší komplicka u celkem tří různých bank.

Není třeba dodávat, že lidé, kteří za zboží zaplatili celkem 360 tisíc korun, se jej nikdy nedočkali. Policisté ovšem oba pachatele vypátrali a v říjnu bylo dívce sděleno obvinění z podvodu a podílnictví, mladík pak skončil ve vazbě. Oběma hrozí až pětileté vězení či peněžitý trest.

Na další podobný případ falešného e-shopu upozornila v prosinci média. Internetový obchod U slona nabízel levnou elektroniku, a ačkoliv na první pohled vypadal solidně (stránky byly dobře graficky zpracovány, obsahovaly obchodní podmínky atd.), zboží zákazníkům nedodával. Rozzlobení zákazníci se pak začali ozývat provozovateli, který byl na stránkách uveden. Brzy se nicméně ukázalo, že tato firma sice existuje, nicméně s obchodem nemá vůbec nic společného. Podvodníci si zkrátka z obchodního rejstříku vypůjčili kontaktní údaje (zřejmě) náhodně vybrané existující společnosti a tu pak na stránkách uvedli jako provozovatele e-shopu. Majitel této firmy na ně proto podal trestní oznámení. Učinit by tak měli i všichni poškození, kteří ve falešném e-shopu U slona nakupovali.

Policie nakonec **shromáždila celkem 79 trestních oznámení**, týkajících se různých falešných e-shopů, které spojoval jeden bankovní účet. Případ se v současné době vyšetřuje. V těchto případech je vždy lepší, když poškození zákazníci čin policii oznámí. Po rozhodnutí soudu totiž mohou mít jednak nárok na odškodnění od banky, u které je falešný účet veden, zároveň může každý další incident dodat policii nové cenné indicie k dopadení pachatelů. Po jejich usvědčení se navíc výše trestu odvíjí také od výše škody, kterou napáchali, proto je vhodné, aby si podvedení zákazníci nenechávali vše pro sebe. Přesto tak řada lidí činí, zřejmě proto, že raději obětuje peníze, než aby kontaktovala policii.

Podle Asociace pro elektronickou komerci (APEK) lze obchodování na internetu obecně považovat za poměrně bezpečné. Vždy se ale vyplatí určitá obezřetnost. Nejlepší je, pokud má kupující sám s internetovým obchodem osobní zkušenosti, anebo dobré reference od jiných zákazníků. Nákup je také bezpečnější v obchodech, které **jsou označené certifikačním logem** APEK, SOAP či Heuréka. **V případě neznámých e-shopů je lepší vyhýbat se platbě předem a dávat přednost například dobírce**. Provozovatelé falešných e-shopů často jinou možnost než platbu předem vůbec nenabízejí, anebo ji výrazně zvýhodní (např. nabídnou dopravu zdarma a slevu 20%; to byl i případ e-shopu U slona).

Zákazník by také **neměl podceňovat obchodní a reklamační podmínky**, které musí být na stránkách uvedeny, a skutečně si je přečíst. APEK dále doporučuje zkontrolovat při převzetí zásilky od dopravce její neporušenost i obsah. Porušenou zásilku je lepší nepřebírat vůbec a raději kontaktovat obchodníka. Totéž platí v případě, že zásilka obsahuje jiné než objednané zboží. Při nákupu zboží přes internet máte u většiny zboží ze zákona právo odstoupit od smlouvy od 14 dnů od jejího převzetí.

V případě, že si nejste zcela jisti důvěryhodností konkrétního internetového obchodu, je možné se s žádostí o radu obrátit přímo na email APEK (info@apek.cz).

Falešný internetový obchod je díky referencím často poměrně rychle odhalen a uzavřen. Pokud se ovšem nepodaří podvodníka včas vypátrat, obvykle si velmi záhy otevře další, pod jiným jménem a s jiným vzhledem, kde opět nabízí zboží, o které je v dané době velký zájem (často elektroniku), za velmi nízké ceny. Do doby, než je nucen obchod uzavřít, obvykle stihne získat pár desítek tisíc korun.

V případě internetových podvodů se ovšem nemusí jednat jen o e-shopy, ale také například **o prodej zboží z druhé ruky**. Jako další modelový příklad může sloužit podvod, jehož obětí se v červenci stala starší žena z Jesenicka. Ta odpověděla na inzerát o prodeji tři roky staré Škody Yeti za 140 tisíc korun. Prodávající se představil jako Španěl, který v ČR před časem pracoval jako inženýr pro firmu ČEZ. Protože se již vrátil domů, vůz dále nepotřebuje, a proto jej prodává.

Přes email se s ženou dohodl, že mu zašle první splátku vozu ve výši 2 700 eur na účet ve Velké Británii. Obratem žena dostala vyrozumění od fiktivní přepravní společnosti, která potvrdila převoz vozu do České republiky. Email obsahoval i sledovací číslo zásilky. Když ale prodejce vůz nedodal a místo toho začal požadovat zbytek ceny, žena zpozorněla a další peníze platit odmítla. V tu chvíli přestal údajný španělský inženýr zcela komunikovat. Podvedená zákaznice si sama na internetu na základě jeho jména našla, že se jedná o podvodníka. V tu dobu již ale přišla o více než 70 tisíc korun a teprve poté případ ohlásila na policii.

Také v těchto případech se tedy vyplatí zvýšená opatrnost předtím, než cokoliv zaplatíte neznámému člověku, aniž byste měli jakoukoliv záruku, že obdržíte nabízenou službu. **Když už nakupujete o neznámého prodejce, vždy se vyplatí si o něm nejdříve na internetu něco zjistit (reference, negativní zkušenosti dřívějších zákazníků)**. Ověřte si také jeho kontaktní údaje, telefonní číslo a adresu (skutečně sídlí tam, kde uvádí?). Pokud prodejce nechce tyto informace poskytnout, raději nic předem neplaťte. Krátký čas navíc strávený hledáním na internetu vám může ušetřit mnoho peněz i starostí.

Aktivity bezpečnostních složek a státní správy

Zřejmě nejvýznamnějším dokumentem, který by měl (nejen) z pohledu státní správy výrazně proměnit sledovanou oblast v ČR, je **Návrh zákona o kybernetické bezpečnosti**, který v průběhu roku 2013 úspěšně prošel meziresortním připomínkovým řízením a dne **2. ledna 2014 jej schválila vláda**. Pokud návrh ratifikuje parlament a podepíše prezident, stane se Česká republika jednou z prvních zemí světa, kde je kybernetická bezpečnost upravována zvláštní právní normou.

Návrh zákona o kybernetické bezpečnosti připravil (ve spolupráci s dalšími státními institucemi) **Národní bezpečnostní úřad, který je na základě usnesení vlády ČR č. 781 ze dne 19. října 2011 gestorem a národní autoritou pro tuto oblast**.

Návrh je primárně zaměřen na zabezpečení informačních a komunikačních systémů veřejné správy a ochranu kritické infrastruktury (KI). Je přitom nutné zdůraznit, že v případě kybernetické bezpečnosti jde o průřezovou oblast, která zasahuje do celé řady různých odvětví KI (např. funkčnost některých klíčových prvků energetické infrastruktury závisí na informačních systémech, které jsou jejich součástí). Cílem zákona bude především určitá standardizace úrovně bezpečnostních opatření a protiopatření (reakce na incidenty) a nastavení funkčního systému hlášení kybernetických bezpečnostních incidentů Národnímu centru kybernetické bezpečnosti, které funguje od září 2012 v Brně.

Návrh zákona vychází ze zásady individuální odpovědnosti za bezpečnost vlastních informačních systémů, přičemž při přípravě návrhu se jeho tvůrci pokoušeli minimalizovat zásahy do práv soukromých subjektů. V praxi se tedy není třeba obávat, že stát bude diktovat, jakým způsobem mají vypadat soukromé informační systémy, jak zaznívalo v diskusích ohledně věcného záměru. Návrh zákona pouze ukládá povinným osobám, jejichž

informační a komunikační systémy jsou pro chod státu důležité, učinit taková opatření, aby nedošlo k narušení bezpečnosti.

Znění Návrhu zákona o kybernetické bezpečnosti tak, jak byl předložen vládě (včetně důvodové zprávy) je ke stažení zde:

http://www.govcert.cz/download/nodeid-577/

K zákonu se váží i další související předpisy, zejména tzv. **vyhláška o kybernetické bezpečnosti** (celý název zní: „vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních protiopatřeních a o stanovení náležitosti podání v oblasti kybernetické bezpečnosti“), kterou v současné době dokončuje meziresortní pracovní skupina, opět pod vedením NBÚ.

Vyhláška vychází zejména z mezinárodní certifikace systému řízení bezpečnosti informací (normy ISO/IEC) a určuje, jaký charakter mají mít organizační a technická opatření vedoucí k zajištění informační bezpečnosti. Vyhláška zejména stanoví obsah, strukturu a formu bezpečnostní dokumentace, obsah bezpečnostních opatření a rozsah jejich zavedení, typy a kategorie kybernetických bezpečnostních incidentů, náležitosti a formu jejich hlášení, příklady reaktivních protiopatření, formu oznamování kontaktních údajů atd.

V souvislosti s Návrhem zákona o kybernetické bezpečnosti bude také třeba upravit **nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury**. K tomuto účelu se schází meziresortní pracovní skupina pod vedení MV-Generálního ředitelství Hasičského záchranného sboru.

Ve sledovaném období došlo ještě k jednomu významnému kroku. Česká republika v létě **ratifikovala budapešťskou Úmluvu o počítačové kriminalitě**, která tak platí od 1. prosince 2013. Jedná se o dokument Rady Evropy, který dosud podepsalo 51 států celého světa, přičemž ratifikace proběhla nejméně ve 40 z nich. Jde o vůbec první mezinárodní smlouvu, která se komplexním způsobem zabývá informační kriminalitou. Její přínos je zejména v tom, že sjednocuje skutkové podstaty trestných činů tak, aby je bylo možné stíhat na mezinárodní úrovni, což je pro fenomén počítačové kriminality, která hranice států nijak nerespektuje, zcela klíčové. Dokument tak poskytuje důležité vodítko pro tvorbu národních předpisů.

ČR budapešťskou Úmluvu podepsala již v roce 2005, ratifikace se ale kvůli některým námitkám zákonodárců i expertů zdržela. Řada činů v dokumentu uvedených byla přitom již v českém trestním zákoníku přítomná. Mezi kriminální činy se podle úmluvy bude řadit třeba nezákonné získání přístupu k počítačovému systému. Úmluva také kriminalizuje například výrobu, dovoz a prodej takových zařízení, která jsou určená k páchání trestné činnosti, například k nezákonnému sledování provozu na počítačových sítích. Stejně tak se kriminalizuje obchod s kódy a přístupovými hesly, která slouží k nepovoleným průnikům do sítí. Dokument pamatuje i na dětskou pornografii, jejíž výroba je už také trestným činem. Zabývá se i porušováním autorských a souvisejících práv.

Na Policejním prezidiu ČR také vznikl dokument s názvem „**Koncepce rozvoje schopností Policie ČR vyšetřovat informační kriminalitu**“, která vzniká jako součást Koncepce boje proti organizovanému zločinu. Tento materiál systémově nastavuje budoucí podmínky pro efektivní odhalování a vyšetřování kybernetických incidentů.

Na počátku roku 2013 bylo také v rámci Europolu vytvořeno **Evropské centrum pro kybernetickou kriminalitu (EC3)**. Centrum by mělo poskytovat podporu pro vyšetřování i stíhání členským státům, školit národní experty a udržovat online databázi kyberkriminality i kybernetický zločinců.

Policejní akademie ČR a Česká pobočka AFCEA za aktivní podpory NBÚ, Národního centra kybernetické bezpečnosti a odborné veřejnosti vydaly **druhé, rozšířené vydání slovníku kybernetické bezpečnosti** doplněné o anglický překlad českého výkladu odborných výrazů. Práce na prvním českém výkladovém slovníku kybernetické bezpečnosti byly zahájeny v roce 2011 členy pracovní skupiny kybernetické bezpečnosti AFCEA ve spolupráci s českými odborníky na kybernetickou bezpečnost. První oficiální verze výkladového slovníku kybernetické bezpečnosti, nad kterou převzal záštitu Národní bezpečnostní úřad a nově vznikající Národní centrum kybernetické bezpečnosti, byla vydána v květnu 2012. Nejnovější vydání je ke stažení zde:

http://www.govcert.cz/download/nodeid-561/

Národní centrum kybernetické bezpečnosti zároveň připravilo dokument, který popisuje doporučený postup, **jak se zachovat v případě DDoS útoku** na instituci nebo společnost v České republice. Zabývá se spoluprací mezi obětí takovéhoto útoku a bezpečnostním pracovištěm CERT/CSIRT. V druhé části podává konkrétní doporučení pro správce komunikačních sítí a další infrastruktury na bázi protokolu IP. Ke stažení zde:

http://www.govcert.cz/download/nodeid-838/

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.

Policejní hotline k hlášení informační kriminality

Od 1. srpna 2012 na základě úkolu Ministerstva vnitra ČR a v souladu s interním řešením centralizace poznatků v rámci informační kriminality v Policii ČR vznikla tzv. "policejní hotline". Jedná se o projekt na zlepšení možnosti veřejnosti při oznamování informační kriminality. Daný projekt má za cíl zefektivnění činnosti v zajištění **zrychlení toku informací o nejzávažnějších formách informační kriminality**, zejména co se týče případů dětské pornografie, extremistické propagandy, počítačového pirátství, podvodů, útoků na data, vydírání, vyhrožování či obchodu s lidmi, od veřejnosti směrem ke specializovaným policejním složkám.

Snahou je docílit efektivnějšího potírání informační kriminality včasnou reakcí na poznatky, adekvátním zajišťováním důkazního materiálu, zajištěním včasné komunikace s provozovateli služeb a poskytovali připojení do sítě internet, a dalšími návaznými aktivitami, které mají za cíl v potlačení protiprávního jednání a adekvátní reakci policejního orgánu směřujícího k identifikaci a postihnutí pachatelů.

V době plánování a vzniku projektu bylo počítáno s přísunem poznatků, jejichž součet byl odhadován maximálně do výše 1500 hlášení ročně a to na základě součtu poznatků do té doby přebíraných tzv. nevládními horkými linkami a různými policejními pracovišti. Právě na ty se obracela veřejnost v době, kdy žádný centralizovaný kontakt pro hlášení informační kriminality neexistoval.

Reálně bylo ovšem v rámci tohoto projektu jen do poloviny října roku 2013 přijato 2988 hlášení a ročně je odhadován přísun cca 4000 až 4500 hlášení. To je průměrně přes 15 hlášení na jeden pracovní den. Navíc se nepotvrdily obavy, že takto získané poznatky budou pro policii vesměs nevyužitelné. Ve skutečnosti se jejich relevance z hlediska služby kriminální policie a vyšetřování pohybuje nad 90%.

Hotline je přístupná online na stránkách www.policie.cz, pod zde zobrazenou ikonou, či přímo na odkazu http://aplikace.policie.cz/hotline/.

Fenomén: bezpečnost mobilních zařízení

Chytré mobilní telefony (smart-phony) jsou zřejmě největším a nejdynamičtěji se rozvíjejícím komunikačním fenoménem současnosti. Podle evropské agentury ENISA (*European Network and Information Security Agency*) překonají smart-phony poprvé v letošním roce klasické stolní počítače (PC) v počtu zařízení, která se denně připojují na internet.

Chytré telefony se ve skutečnosti od PC zase tolik neliší – jsou vybavené výkonnými procesory, kapacitní pamětí, operačním systémem, složitými programy, připojením k internetu atd. **Smart-phone je vlastně daleko více přenosný počítač než telefon (v původním smyslu slova), a tudíž se na něj vztahují všechna bezpečnostní rizika, která jsou známá u klasických stolních počítačů, plus řada dalších, které pramení z jeho mobility a dalších specifických vlastností.** To, že tyto přístroje stále označujeme jako „telefony" (tj. zařízení určená primárně k hlasové komunikaci) je s každým dalším rokem více a více zavádějící a podle všeho má tato zdánlivá lingvistická drobnost i své konkrétní dopady. Jak totiž ukazují průzkumy, **běžní uživatelé si důsledky technologického vývoje dosud nestačili v plné míře uvědomit a ke svým smart-phonům přistupují stejně, jako kdyby se jednalo o staré analogové mobily z 90. let, u kterých byla bezpečnostní rizika zcela jiného charakteru**.

Z výsledků ankety společností AVG a Ponemon Institute vyplývá, že **pouze 29% vlastníků mobilních telefonů má na svém přístroji instalovaný antivirový program (ať již placený či neplacený), anebo jeho instalaci alespoň zvažuje**. To je dost alarmující číslo, které je velmi pozoruhodné i v tom ohledu, že v případě klasických PC je počet zařízení vybavených nějakým antivirovým softwarem podle odhadů přes 80% (podle zprávy McAfee to bylo celosvětově 83% v roce 2012, poměr vůči mobilním telefonům je tedy velmi znatelný).

Zatímco u klasických stolních počítačů už si lidé zvykli používat určitý stupeň ochrany, v případě smart-phonů je úroveň zabezpečení obecně daleko menší, což z nich činí ideální cíl pro hackery, stalkery a další individua, obdařená nekalými úmysly. S pokračujícím přesouváním většího a většího objemu dat a služeb na mobilní zařízení, která stále častěji slouží i k provádění finančních transakcí či k zasílání citlivých informací, se **přitažlivost smart-phonů pro kriminální živly jen zvyšuje**, a to prozatím bohužel rychleji, než povědomí uživatelů o základních bezpečnostních opatřeních, která mohou riziko zneužití jejich mobilních zařízení výrazně snížit. I to je jedním z důvodů, proč byla na loňské bezpečnostní konferenci Black Hat mobilní zařízení označena za největší bezpečnostní výzvu nadcházejících několika let.

Následující text shrnuje hlavní rizika plynoucí z užívání mobilních telefonů a také upozorňuje na způsoby, jak tato rizika zmenšit či eliminovat z hlediska běžného uživatele. Přestože to tak může z některých pasáží vyznívat, cílem není kohokoliv od užívání smart-phonů odradit. Podobně jako v případě jiných přelomových technických fenoménů se ostatně zřejmě ani nebude možné využívání chytrých telefonů dlouhodobě vyhýbat, protože se postupně stávají důležitou součástí běžného fungování společnosti, podobně jako třeba elektřina či internet. Ovšem jako každá nová technologie přináší i tato řadu negativních dopadů a bezpečnostních rizik, o jejichž existenci je dobré přinejmenším vědět.

Rizika se pochopitelně netýkají jen mobilních telefonů. Velmi ohrožené jsou například tablety, u kterých je úroveň zabezpečení obecně ještě nižší než u smart-phonů a mnoho lidí na ně ukládá značné množství pracovních dat.

V nejbližší budoucnosti to budou právě mobilní zařízení, která budou představovat hlavní bezpečnostní výzvu. Dá se nicméně předpokládat, že úroveň zabezpečení se i u mobilů bude postupně přibližovat stolním počítačům, přestože některá specifická rizika dále přetrvají. S každou další generací smart-phonů je zabezpečení obecně lepší, objevují se ale také nové metody útoků a nové hrozby.

Obecně se dá tento trend přirovnat k vývoji bezpečnosti u osobních automobilů. Projížďka velmi starým vozem byla z dnešního pohledu velmi riskantní záležitostí – absence airbagů, deformačních zón, ABS atd. Moderní auta jsou v tomto ohledu výrazně bezpečnější, na druhou stranu jsou také výkonnější, rychlejší a provoz na silnicích je mnohem hustší. Přesto se dá říci, že statisticky se jak jízda autem, tak používání mobilních telefonů pomalu posouvá směrem k větší bezpečnosti, třebaže se vždy bude jednat o nikdy nekončící boj. Zvláště proto, že trend jednoznačně směřuje k přesunu od stolních počítačů k mobilním zařízením.

Možné způsoby nákazy mobilního zařízení malwarem

Pokud je chytrý telefon ve skutečnosti vlastně počítačem, může se také, jako každý jiný počítač, nakazit počítačovým virem. **Na začátku minulého roku existovalo odhadem asi 50 tisíc různých druhů malware, který napadal mobilní telefony. Pro tento a příští rok se všeobecně očekává jeho exponenciální nárůst, takže v budoucnu nejspíš početně překoná útoky na klasická PC**, kde je „trh se škodlivým softwarem“ daleko více nasycen a už neroste zdaleka tak dynamicky, jako v průběhu uplynulé dekády. **Většina tvůrců počítačových virů se zkrátka nově bude soustředit právě na mobily.**

Škodlivého software pro mobilní zařízení existuje celé řada, s různými dopady pro uživatele, přičemž některé z nich budou popsány v následujících oddílech. Tato podkapitola se soustředí především na to, jakým způsobem se může malware do mobilního zařízení dostat.

Ty nejzákladnější způsoby jsou stejné jako u kteréhokoliv jiného počítače. V případě klasických PC se nejčastěji přístroj nakazí prostřednictvím emailu, konkrétně pak většinou metodou **phishingu**. Uživateli přijde nevyžádaný email, ve kterém je obvykle příloha (program, dokument pdf atd.) nakažený virem, případně odkaz na falešnou stránku nějaké známé instituce. Sofistikovanější metodou je tzv. spear phishing, kdy útočník cílí přímo na konkrétní oběť a použije v emailu údaje, které si o ní zjistil (ať již na internetu nebo jinde) a někdy dokonce zfalšuje i emailovou adresu odesílatele, takže si příjemce myslí, že mu píše někdo známý (tzv. **spoofing**). Spear phishing je většinou velmi úspěšný a tímto jednoduchým způsobem se i do zabezpečených sítí státní správy a velkých firem dostaly pokročilé špionážní viry jako Red October či MiniDuke.

Staré značně amatérské emaily psané mizernou češtinou z automatického překladače, ve kterých se příjemce dozvěděl, že se stal výhercem pohádkové částky, pro jejíž vyzvednutí musí kliknout na konkrétní odkaz, jsou už dnes vesměs překonané, protože většina uživatelů už se je naučila ignorovat (přesto je až udivující, jak byly účinné). V dnešní době se objevují mnohem sofistikovanější způsoby – např. email z adresy vašeho nadřízeného (nebo adresy velmi podobné), s příslušnou hlavičkou, který vás stručně upozorňuje na důležitý dokument v příloze, jehož název se týká vaší běžné práce. Všechny informace potřebné pro vytvoření takového podvodného emailu není problém z internetu zjistit a statisticky je prokázané, že přílohu z takto formulovaného mailu otevře drtivá většina zaměstnanců.

Existuje řada dalších běžných způsobů, jak se může PC nakazit malwarem (podvržené internetové stránky, připojení k nakaženému zařízení atd.), tento text ale nemá prostor se jim věnovat, protože je primárně zaměřen na mobilní telefony. Postačí tedy zdůraznit, že váš **chytrý telefon se může nakazit virem v podstatě všemi způsoby, jakými se může nakazit váš stolní počítač či notebook. Při práci s ním byste tedy měli dodržovat stejné bezpečnostní zásady, např. mít nainstalovaný aktualizovaný antivirový program**.

V případě chytrých telefonů se k výše uvedeným formám napadení připojují ještě další, specifické, kterými jsou např. **nakažené mobilní aplikace** a **podvodné SMS**. Falešné SMS se objevují méně často a jejich princip je stejný jako u falešných emailů – obvykle obsahují odkaz na stránku s virem. Je ale třeba si na ně dávat velký pozor, protože například jeden z nejslavnějších virů Eurograbber (o kterém bude ještě řeč, protože napáchal obrovské finanční škody desítkám bank) použil k prolomení dvoufaktorové autorizace u internetového bankovnictví mimo jiné právě SMS s internetovým odkazem.

Jsou to ale právě aplikace, které jsou v současnosti nejčastějším způsobem, jakým se do smartphonů dostává škodlivý software. Zde fungují v zásadě dvě metody, jak virus rozšířit:

1. vyvinout a distribuovat celou nakaženou aplikaci
2. využít chyby v zabezpečení některé z populárních aplikací a opatřit jí virem

Velmi často dojde k nákaze malwarem po návštěvě falešného, případně neověřeného app-storu. Hackeři zde využívají nepozornosti uživatelů, kteří se mohou snadno splést např. při zadávání adresy internetového obchodu, a tak kromě oficiálního Google Play existuje např. falešný Google Plays atd. Na těchto stránkách obvykle naleznete řadu nejpopulárnějších aplikací známých z oficiálních obchodů, které ale navíc obsahují malware.

Stránek imitujících velké obchody jako je právě Google Play a Apple App Store stále přibývá, ve skutečnosti ale **infikované aplikace pronikají ve stále větší míře i do oficiální distribuce**. Při množství aplikací, které se v těchto obchodech prodávají a jejich rychlé obměně, je prakticky nemožné uhlídat, zdali některá z nich neobsahuje také části se škodlivým kódem. I v případě, že se nákaza odhalí, stane se tak obvykle v případě, kdy si již aplikaci stáhly tisíce uživatelů. Oficiální distributoři proto vymýšlí způsoby, jak šíření malwaru zabránit – je to např. skrze tzv. **kill-switch**, který automaticky smaže konkrétní aplikaci na dálku na všech zařízeních, na které byla nainstalována, případně snaha přesunout většinu aplikací do tzv. sand-boxů, kde jsou oddělené od dat a dalších funkcí přístroje uživatele.

Známými příklady úspěšného malwaru z poslední doby mohou být trojské koně **Gemini** (nakazil desetitisíce uživatelů, především v Číně, kteří stahovali hry zdarma z neoficiálních stránek) a **DroidDream.** U něj bylo zaznamenáno přes 200 tisíc nakažení během několika dní, napadal systémy Android a objevil se i v oficiálním obchodě, kde byl součástí populárních aplikací, jejichž jméno bylo mírně změněno tak, aby si toho uživatelé nevšimli.

Bohužel, dokonce ani v případě, že si jako uživatelé dáváte maximální pozor, nemusíte zneužití svého přístroje zcela zabránit. To například v případě, kdy je malware již přímo součástí přístroje, který si koupíte od výrobce. Takové zneužití bývá velmi obtížně odhalitelné, pro běžného uživatele je to pak téměř nemožné (v případě špionážního malwaru se dá např. měřit odesílaná data, ale i tyto údaje může mobil falšovat). Tento typ nákazy se někdy objevuje u přeprodávaných telefonů, v bazarech a u přístrojů sestavených z neoriginálních dílů.

Samostatnou kapitolou jsou pak tzv. backdoor, které do přístroje dodá samotný výrobce, a to např. na základě požadavků zpravodajských služeb, či za účelem průmyslové špionáže. Velký problém, na který již nějakou dobu upozorňují zpravodajské služby západních zemí, jsou zejména **přístroje vyráběné v Číně**, u kterých byla tato „zadní vrátka“ již několikrát odhalena.

Například Kanada tak již zcela vyřadila čínské výrobce z tendrů na zakázky komunikačních technologií pro státní správu, USA se zase zbavují čínských komponentů ve svých zbraňových systémech. Na černou listinu se dostaly zejména firmy Huawei a Lenovo, nad nimiž se vznáší podezření ze spolupráce s čínskými zpravodajci.

Situace je ale ve skutečnosti méně jednoznačná, než se na první pohled zdá. Čínské komponenty totiž obsahuje většina mobilních telefonů bez ohledu na jejich výrobce (všechny velké telekomunikační firmy mají množství dodavatelů po celém světě). Navíc instalace zadních vrátek není rozhodně jen výsadou Číny. Západní země se netají, že backdoor inkorporované přímo do přístrojů využívají, ale pouze v případech podezření na ohrožení národní bezpečnosti (např. kvůli hrozbě terorismu). Čína je obviňována zejména z toho, že postupuje nad rámec této „standardní praxe" tím, že „backdoor" využívá k průmyslové špionáži, ke špehování soukromého sektoru a získávání ekonomických výhod pro vlastní firmy. Ty tak ušetří miliardy dolarů za vývoj a kopírují západní produkty často ještě dřív, než se vůbec dostanou na trh. Čínské produkty jsou tedy některými analytiky vnímány jako ohrožení, především pro byznys a bezpečnostní a ekonomické složky státní správy.

Riziko kompromitace dat

Riziko ztráty, krádeže či kompromitace dat je u mobilních zařízení obecně vyšší než u klasických PC. V tomto smyslu je možné rozlišit několik základních možností, jak může k ohrožení dat u chytrého telefonu dojít:

1. ztráta či odcizení samotného přístroje
2. nakažení špionážním malware
3. nezabezpečené bezdrátové připojení

Vánoce – svátky míru a hackerů

Statistiky z konce roku 2013 opět potvrdily fenomén zvýšeného počtu phishingových útoků v období Vánoc a přelomu roku. Jedná se hlavně o zavirovaná novoroční přání, která nemusí přicházet jen z neznámých adres, ale také od přátel a známých, jejichž počítač byl již virem napaden. Malware se šíří také prostřednictvím zasílaných nabídek na výhodné předvánoční nákupy, tipy na dárky či novoroční slevy. Koncem roku se objevilo také velké množství emailů, které se vydávají za zprávy České pošty. Ty vyzývají adresáta k vyzvednutí nedoručené zásilky či nabízejí odkaz na stránku, kde je možné sledovat její pohyb. Odkazy v těchto emailech jsou podvržené a po kliknutí na ně se uživatelům do počítače dostane nebezpečný malware. Přesto slaví tento typ útoků značné úspěchy, protože před Vánoci si mnoho lidí nechává zasílat poštou objednané zboží a email od doručovatelské společnosti jim tak nepřijde podezřelý. V minulosti byl tento typ (zejména) emailového phishingu snáze odhalitelný díky špatné češtině, i to se ale v poslední době mění. Nemalý počet zpráv je psán přímo českými hackery, případně zahraniční emaily překládají za příslušnou provizi rodilí Češi.

Riziko ztráty či krádeže je u telefonu pochopitelně výrazně vyšší než u stolního počítače (ale i vyšší než o notebooku). Je proto vhodné dodržovat několik základních bezpečnostních pravidel. Tím prvním a nejobecnějším **je vnímat mobilní telefon jako prostředí náchylné ke kompromitaci dat**. To znamená zvážit, které soubory či informace je nutné mít v mobilním zařízení uložené, a které jsou příliš citlivé na to, abych riskoval jejich ztrátu či vyzrazení. To se týká zejména **služebních mobilních telefonů, které jsou využívány také pro soukromé účely**. Jedná se o poměrně běžnou praxi, využíváním k různým účelům se přitom například riziko infekce škodlivým softwarem výrazně zvyšuje. Proto by lidé, kteří musí mít z pracovních důvodů ve svém telefonu velmi citlivá data, měli v ideálním případě používat dva různé přístroje.

Podobně je dobré zvážit, zda je opravdu nezbytně nutné mít skutečně citlivá data trvale přítomná v mobilním přístroji a v případě, že ano, v jaké formě a je tam mít uložené. Také mobilní telefony nabízejí možnosti šifrování, které jsou volně stažitelné. Mnoho lidí má také v telefonu **uložena různá hesla, PIN, přístupové údaje k internetovému**

bankovnictví atd. To je obecně velmi rizikové, třebaže vzhledem k mobilitě přístroje poměrně praktické. Pokud to uživatel skutečně považuje za nezbytné, je dobré tato data buď elektronicky šifrovat (pomocí k tomu určených programů), anebo je alespoň uvádět skrytě (např. PIN může být součástí telefonního čísla v dlouhém seznamu kontaktů, což hackerovi jeho identifikaci ztíží, podobně heslo do počítače inkorporovat do delšího textu atd.).

Tato opatření ale v případě úplné ztráty či cíleného odcizení telefonu obvykle nestačí. Zloději či nálezci ztíží přístup již to, pokud je telefon zamčený a chráněný nějakou formou autorizace (PIN atd.). Přístroj je dobré mít nastaven tak, aby se po určité době automaticky zamkl (čím je tato doba kratší, tím obecně snižujete riziko, že bude s vaším telefonem manipulováno). Je také možné zařídit, aby se po určitém počtu neúspěšných pokusů telefon automaticky zformátoval, a zničil tak veškerá data (která je pak ovšem nutné mít zálohována jinde). Tento tzv. **auto-wipe** je možné provést i na dálku (remote-wipe), pokud si na svůj přístroj tuto funkci nainstalujete. Některé placené aplikace jdou při ztrátě mobilních telefonů ještě dál. Je například možné zapnout na dálku GPS a zjistit, kde se váš ukradený telefon právě nachází. Existují i další programy určené k odhalení pachatele krádeže, např. takový, který po neúspěšném pokusu o odemknutí telefonu zloděje vyfotí a fotografii zašle na předem zadaný email.

Telefon s citlivými daty pokud možno nedávejte do ruky nikomu cizímu. Na konferenci Black Hat například zaznělo, že je při důležitých obchodních jednáních po účastnících často požadováno, aby své mobilní telefony před vstupem do místnosti odevzdali. Jedná se o poměrně běžnou praxi, kterou se má zabránit např. odposlechu. V některých případech ale následně došlo ke **kompromitaci těchto zařízení** a jejich nakažení špionážním malware. Bezpečné v tomto směru prý nejsou ani hotelové trezory, a to zejména v asijských a afrických zemích. Pokud je to možné, je lepší mít telefon s citlivými daty stále při sobě.

U veřejně činných osob hrozí nejen krádež dat, ale možné je pochopitelně i jejich přidání. V přístroji politika či obviněného podnikatele se tak mohou nalézt kompromitující materiály, které jej usvědčují ze spolupráce se zločinci, z nevěry, z krádeže atd. Připojení se k **nezabezpečenému bezdrátovému připojení** (např. bezplatná wi-fi) je dalším ze způsobů, který může vyústit v krádež dat z mobilního telefonu. Bezplatné bezdrátové připojení je dnes v kavárnách, restauracích či na letištích poměrně běžným jevem a lze se s nimi setkat stále častěji. Stále častější jsou bohužel také sítě falešné, skrz které může hacker poměrně snadno získat přístup k vašim datům. Proto je lepší využívat jen ověřené a zabezpečené bezdrátové připojení.

Rizika ztráty soukromí

Ještě před dvaceti lety bylo sledování a odposlouchávání lidí značně rizikové a vyžadovalo poměrně dost úsilí a prostředků. Pro odposlech utajovaného jednání bylo potřeba se dostat do zabezpečeného objektu a nainstalovat tam záznamové zařízení. Pokud jste se chtěli dozvědět, kam daná osoba cestuje a co dělá, museli jste ji fyzicky sledovat. S nástupem chytrých telefonů lze toto všechno provádět z bezpečí vlastního domova a řadu z těchto „špionážních“ činností dokonce zvládne i průměrně technicky zdatný člověk. **Mobil ve vaší kapse totiž může útočníkovi snadno nahradit štěnici i sledovací zařízení**.

Některé funkce současných smart-phonů totiž dávají někomu, kdo si o vás přeje zjistit co nejvíc, skutečně netušené možnosti. Je dobré si připomenout, co takový pokročilý špionážní malware mimo jiné dokáže. Zdaleka zde totiž nejde jen o možnost krádeže dat, uložených v mobilu, případně záznamů vašich hovorů. Pokud útočník ví, že v určitou hodinu máte důležitou obchodní schůzku a váš přístroj je nakažen příslušným špionážním malwarem, může na dálku zapnout mikrofon či kameru ve vašem mobilu a celé utajované jednání si nahrát a online odeslat.

Odposlech je možné dělat i uskutečněním klasického telefonního hovoru z vašeho čísla na číslo útočníka. Při pohledu na mobil přitom nic z toho nemusíte vůbec poznat – všechno se odehrává na pozadí a na displeji se nic nezobrazuje. Běžnou manipulací s telefonem tedy nemáte šanci cokoliv zjistit. Jistotu, že váš mobil během jednání neslouží jako štěnice, budete mít zřejmě jen tehdy, pokud jej vypnete a vyjmete baterii (případně si jej na schůzku vůbec nevezmete). Další možností je nákup speciálního příslušenství. Nový americký produkt nazvaný OFF Pocket vypadá jako běžný obal na mobilní telefon, ve skutečnosti má ale za úkol ochránit zařízení např. před datovými odposlechy a zajistit tak uživatelům potřebné soukromí. Kapsa je totiž vyrobena ze speciálního materiálu, který přístroj fyzicky izoluje od mobilního signálu, wi-fi, GPS i dalších možností bezdrátového přenosu. Nelze tak například zjistit Vaši polohu, ani na dálku získávat z přístroje data. Výrobce uvádí, že možnost je určena pro ty, kdo chtějí zabránit narušení jejich soukromí či sledování, případně se chtějí prostě jenom „úplně odpojit“. I vypnutý telefon totiž teoreticky může sloužit jako sledovací zařízení.

Každý sedmý Čech přišel v roce 2013 o svá mobilní data

Podle průzkumu ruské společnosti Kaspersky Lab, která patří mezi největší soukromé firmy v oblasti bezpečnostního softwaru, přišlo o veškerá svá data uložená na mobilním zařízení (zejména chytré telefony a tablety) víc než 13% českých uživatelů. V 8% případů za to mohlo nenávratné poškození přístroje, 3% lidí zařízení ztratilo a 3% bylo odcizeno. Tato statistika je varovná zejména z toho důvodu, že stále větší počet lidí si na svůj mobilní telefon ukládá velmi citlivá data. Více než polovina zařízení obsahuje nezabezpečenou soukromou emailovou korespondenci, třetina pak korespondenci pracovní. Hesla k emailovým účtům a účtům na sociálních sítích lze nalézt na 16% mobilů a 19% tabletů, 8% procent smartphonů pak obsahuje hesla k internetovému bankovnictví. Kaspersky Lab prováděl tento průzkum v celkem 19 zemích.

Moderní telefony jsou dnes také téměř všechny vybaveny GPS, které se dá rovněž na dálku vypínat a zapínat, takže je možné získat přesnou polohu i záznam pohybu sledované osoby s přesností na metr. V kombinaci např. s daty z mobilního kalendáře získáte představu nejen, kde daný člověk právě je, ale také kdy a kde bude. Zajímavé je, že všechny tyto funkce umožňují na dálku i běžně dostupné aplikace - přesněji řečeno, umožňují je pro váš vlastní telefon, hackerovi se ale může podařit nahrát jejich modifikovanou verzi i na cizí přístroj, obvykle prostřednictvím výše uvedených klasických cest nakažení škodlivým kódem.

Dobrým příkladem, co všechno lze o činnosti člověka z jeho telefonu zjistit, je nová placená aplikace s názvem **Jigsaw**, kterou si můžete pro svůj telefon zakoupit v internetovém obchodě. Vyvinuli ji na univerzitě v New Hampshire ve spolupráci s Nokia Research Center v kalifornském Palo Alto. Je určena zejména lidem, kteří jsou posedlí možností sdílet své denní aktivity na sociálních sítích jako je Facebook. Jigsaw jim tuto činnost výrazně usnadňuje, protože z pohybů mobilu pozná, co právě dělají a v závislosti na nastavení ji automaticky postuje jejich přátelům. Díky akcelerometru a gyroskopům uvnitř smartphonů (které se jinak využívají např. při hrách či při překlápění obrazovky) tato aplikace určí nejen to, zdali právě běžíte či jdete (pozná třeba, jestli jdete do kopce či s kopce, do schodů, nebo se otáčíte), ale dokonce i to, jestli máte při chůzi umístěný mobil v kapse u kalhot nebo u saka. Výzkumníci změřili vzorce několika desítek běžných pohybů v závislosti na umístění mobilu, a aplikace tak velmi přesně pozná vaši současnou činnost.

Tyto informace vás mohou znepokojit i v případě, že nejste ani politik, ani podnikatel či příslušník zpravodajské služby. **V USA bylo již např. odhaleno několik případů, kdy si zloději aut a vykradači bytů tipovali svoje oběti právě prostřednictvím údajů získaných ze sociálních sítí a mobilních telefonů**. Člověk nemusí být nutně hacker, aby toho o vás mnoho zjistil, zvláště když máte tendenci tyto informace sami sdílet. **Mnoho lidí používá například aplikace, které při sportu (běhu, jízdě na kole) zaznamenávají vaši trasu a polohu. Pokud neprovedete příslušné změny v nastavení, mohou tyto vaše aktivity vidět také všichni ostatní majitelé těchto aplikací** (lidé se totiž rádi chlubí svými sportovními výkony). Není pak velký problém zjistit, že každý den v určitý čas budete běžet svou oblíbenou trasu, která vám obvykle trvá 54

minut, během kterých nebude nikdo doma. Sledování online polohy ostatním umožňují i jiné než sportovní aplikace (Whatsapp apod.). Členové jednoho zlodějského gangu v USA vypověděli, že si své oběti vybírali právě na základě kombinace údajů získaných z GPS mobilů a fotek na facebookových profilech. Z těch bylo pro změnu možné se dozvědět jaké cennosti daný člověk vlastní, jak přibližně vypadá jeho byt, že je právě na dovolené, že má psa atd.

Stahované aplikace jsou dalším ze způsobů, jak se o vás může někdo dozvědět více, než byste sami chtěli. Řada aplikací totiž při instalaci požaduje přístup k takovým funkcím, které pro svou běžnou činnost ve skutečnosti vůbec nepotřebují – k vašim telefonním kontaktům, k internetu, k SMS zprávám atd. Uživatel s tím instalací dané aplikace uděluje souhlas. V lepším případě pak prodejce takto (legálně) získané údaje využije pouze k marketingovým účelům (získá např. množství telefonních čísel vašich přátel, se kterými zřejmě sdílíte společné zájmy atd.). V současné době zatím většinou není možné si vybírat, jaké funkce aplikaci umožníte, a které jí naopak chcete znepřístupnit (o takové úpravě, která povede k větší ochraně spotřebitele, velcí distributoři v současnosti jednají). Jako uživatel máte zatím jedinou šanci – buď program nainstalovat jako celek, anebo jej neinstalovat vůbec. U těch aplikací, které požadují nesmyslná práva nemající přímou souvislost s jejich běžnou funkcí, je zřejmě lepší zvolit onu druhou možnost.

Celosvětový průzkum společnosti TrustPort, který probíhal ve 30 zemích, bohužel ukázal, že uživatelé softwaru se licenčními podmínkami prakticky nezabývají a podepíší v podstatě cokoliv. Podmínky licenční smlouvy a seznam oprávnění čte údajně zhruba jen 10% uživatelů. Smlouva přitom může obsahovat důležité informace související s nakládáním s osobními údaji, např. umožnuje odesílání soukromých dat na vzdálené cloudové úložiště bez předchozího upozornění. Přitom je celých 79% dotázaných spokojeno s úrovní bezpečnosti svých smart-phonů.

Riziko ztráty peněz

U obyčejných uživatelů ovšem nejčastější důvod napadení jejich mobilního zařízení nespočívá ve snaze je sledovat, ale připravit je o jejich finance. Vůbec nejběžnější formou škodlivého softwaru, který napadal uživatele mobilních telefonů v minulých letech, byl tzv. **diallerware**. Ten bez vašeho vědomí píše nebo volá na zpoplatněná telefonní čísla (nejčastěji skrytě odesílá tzv. prémiové SMS). Napadený uživatel pak něco takového zjistí až z velmi tučného účtu za telefon – operátoři v těchto případech obvykle žádné reklamace neuznávají. **Různé formy diallerware tvořily v roce 2012 až 40% celkového objemu malware u mobilních telefonů**.

Další formy virů se snaží zjistit vaše údaje při placení online kreditní kartou či prostřednictvím internetového bankovnictví. Z těchto důvodů **lze obecně považovat finanční transakce prováděné přes mobil za o něco rizikovější než z klasického PC**. Nástup chytrých telefonů také způsobil prolomení té dosud zřejmě vůbec nejspolehlivější ochrany při internetovém placení, zasílání autorizačního SMS kódu.

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. 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.

Tato možnost se přitom objevila právě až u nových „chytrých“ telefonů – staré analogové mobily byly z hlediska dvoufaktorové autorizace několikanásobně bezpečnější (zdá se totiž, že v jejich případě k prolomení nikdy nedošlo).

Konec prémiových SMS v USA?

Zajímavá zpráva přišla v listopadu ze Spojených států. Jak jsme již informovali v předchozích Situačních zprávách, prémiové SMS byly jedním z nejčastějších způsobů, jak uživatele mobilních telefonů podvodně připravit o peníze.

Objem podvodů a nekalých praktik v této oblasti mobilních služeb dosáhl takových rozměrů, že regulátoři ze 45 amerických států začali usilovat o úplné zrušení této služby. Podle odhadů totiž každý rok přišli američtí uživatelé mobilních telefonů **díky nevyžádaným prémiovým SMS v přepočtu o více než 40 miliard korun** (2 miliardy dolarů). Podle průzkumu z května 2013 bylo **až 60% celkového objemu prémiových služeb zneužito k podvodům** a neoprávněným operacím. Tato čísla nakonec přiměla operátory jednat, třebaže to rozhodně nebylo v jejich finančním zájmu (z prémiových služeb si účtovali provize i ve výši 50% ceny).

V poměrně dlouho vedené diskusi nakonec nastal koncem roku 2013 zásadní průlom, když čtyři největší američtí operátoři (Verizon, Sprint, AT&T a T-mobile) oznámili, že službu až na drobné výjimky přestanou poskytovat.

Mezi prémiové služby však patří také dárcovské SMS (v ČR známé zejména z časů povodní či velkých živelných katastrof v jiných zemích) a v USA také časté zprávy na podporu volebních kampaní. V těchto případech se pochopitelně o podvody nejedná a společnosti Verizon a T-mobile tyto služby v plném rozsahu zachovají (AT&T ponechá pouze charitativní programy).

V tuto chvíli se nezdá, že by podobné razantní kroky plánovali i čeští operátoři, a to navzdory tomu, že také v České republice jsou s prémiovými službami problémy. Známá je například kauza společnosti DIMOCO. Na ni si stěžovali desítky spotřebitelů s tím, že od firmy obdrželi nevyžádané prémiové SMS. Účet za mobilní telefon jim tak mnohdy narostl až o několik set korun. Český telekomunikační úřad nakonec na tuto společnost se sídlem v Rakousku podal trestní oznámení. Společnost ovšem vinu odmítá. Jedním z možných řešení je si prémiové služby u svého operátora zcela zablokovat.

10 doporučení pro zvýšení bezpečnosti

Doporučení 1: Každý uživatel smart-phonu by měl mít na svém zařízení nainstalován antivirový program (v app-storech je jich k dispozici velké množství a některé verze jsou zdarma) a dodržovat stejné zásady bezpečnosti, jaké se doporučují u běžného PC (neotevírat podezřelé a nevyžádané emaily, nenavštěvovat rizikové internetové stránky, dávat si pozor na ty falešné atd.). Nainstalovaný antivirus by měl také pravidelně aktualizovat.

Doporučení 2: Stahovat a nakupovat aplikace pouze v oficiálních obchodech (např. Google Play či Apple App Store) a pokud možno se vyhýbat neautorizovaným a málo známým app-storům. Také si dávat pozor, zda se opravdu nacházíte na stránce oficiálního obchodu, a ne na její věrné napodobenině. Ani tak sice riziko stažení infikované aplikace nezmizí, ale výrazně se sníží, navíc roste pravděpodobnost, že vás distributor v případě odhalení malwaru na rizikovou aplikaci upozorní. Je také obecně lepší dávat přednost aplikacím s dobrým hodnocením od velkého množství uživatelů, které sice lákají hackery ke zneužití, ale mají obvykle lepší úroveň zabezpečení. Je rovněž nutné si aplikace (i operační systém telefonu) pravidelně aktualizovat, protože aktualizace často obsahují bezpečnostní záplaty a vylepšení.

Doporučení 3: Kupovat nejlépe nové přístroje u autorizovaných prodejců. Při nákupu v bazarech je větší riziko pořízení zařízení, které již obsahuje malware. V případě nákupu služebních přístrojů pro státní správu či firmy s chráněným know-how je možné požadovat po výrobci záruky, že žádná z klíčových komponent nepochází z rizikových zemí. Takové požadavky mohou být ovšem těžko splnitelné, případně mít zásadní vliv na cenu produktu. Pozor je nutné si dávat také na různé dárky a pozornosti – není nic snazšího než darovat na jednání člověku či instituci, která je předmětem vašeho zájmu, drahý a krásný mobilní přístroj (případně flash disk, tablet) s ukrytým špionážním malwarem.

Doporučení 4: Nenahrávejte na mobilní zařízení žádná citlivá a zneužitelná data, pokud to není opravdu nezbytné. Pokud to nezbytné je, používejte k jejich ochraně nějakou formu šifrování, v závislosti na důležitosti chráněných dat. Nastavte si telefon tak, aby se při nečinnosti rychle uzamkl a PIN či heslo k němu nenoste nikdy společně s přístrojem. Je možné používat i výše uvedené programy k identifikaci útočníka či ke zničení dat v případě odcizení telefonu. Data uložená v mobilu si vždy zálohujte i na jiném médiu.

Doporučení 5: Nepřipojujte se k neznámým a nezabezpečeným bezdrátovým sítím (wi-fi). Bezdrátové připojení je obecně rizikovější formou komunikace (i známá síť může být napadena hackerem), proto přes veřejné wi-fi raději nikdy neposílejte citlivá data, nepřihlašujte se do systému elektronického bankovnictví atd.

Doporučení 6: Hlídejte si své soukromí a nedovolte, aby se váš telefon stal nástrojem ke špehování vaší osoby. Sdílení vaší polohy prostřednictvím GPS je obvykle možné aplikacím zakázat. GPS je také dobré mít po celou dobu, kdy ji právě nepoužíváte, vypnutou. Krom toho, že ztěžujete jiným osobám lokalizovat vaši polohu, tím také šetříte baterii. Přistupujte s rozvahou ke sdílení údajů o vaší činnosti prostřednictvím svého mobilního telefonu.

Doporučení 7: Věnujte pozornost přístupovým právům, které po vás vyžaduje instalovaná aplikace. Většina lidí je bez povšimnutí odklikne, čímž často dává developerům aplikací nepřiměřené pravomoci legálně získávat vaše soukromé údaje.

Doporučení 8: Pokud se svého telefonu chcete zbavit (např. jej prodat či odevzdat), proveďte důkladný výmaz všech dat (nezapomeňte ani na přídavnou paměťovou kartu). Existují nicméně technologie, jak obnovit data i ze zformátovaného zařízení, takže úplnou jistotu bude mít pouze při fyzickém zničení všech paměťových součástí přístroje. To se samozřejmě vyplatí zejména těm lidem, kteří měli na svém telefonu skutečně citlivá data. Varováním může být například případ aljašské guvernérky a jedné z kandidátek do amerického prezidentského úřadu Sarah Palinové. Její mobily po neúspěšné volební kampani skončily v bazaru, aniž by si dal její štáb práci s vymazáním dat. Její emailová korespondence a další zprávy osobního charakteru se následně objevily na internetu, což tuto političku značně poškodilo.

Doporučení 9: Odesílání prémiových SMS a volání na placené linky je možné si u svého operátora zakázat. Ale pozor – zabráníte tím sice zneužití svého mobilu, ale připravíte se o možnost tyto služby využívat (včetně např. odesílání dárcovských SMS při povodních, SMS jízdenky do MHD apod.). Je ale například možné vypsat konkrétní čísla, na které bude tato služba povolena. Jedinou další ochranou je zabránit nakažení vašeho telefonu diallerwarem a pravidelné průběžné sledování účtu za telefon (např. nastavením limitů, po kterých budete vaším operátorem upozorněni, či bude váš účet zablokován).

Doporučení 10: Mimořádně opatrní byste měli být při využívání mobilu k online placení. To se ani tak netýká nové technologie, při které bude možné mobil přikládat k terminálu podobně jako platební kartu. Spíše jde o internetové bankovnictví. Pokud je totiž virem nakaženo jen vaše PC, po přihlášení do online bankingu získá útočník pouze vaše přihlašovací údaje, ale pro provádění transakcí nebude mít příslušný SMS kód. Pokud je ale malwarem nakažen váš mobil, přihlášením k této službě získá útočník vše, co potřebuje k tomu, aby převáděl peníze na vašem účtu.

Exkurz: Cryptolocker

Ani České republice se nevyhnuly případy napadení novým červem Cryptolocker, který po uživatelích požaduje výkupné výměnou za dešifrování dat. Cryptolocker je mezinárodně rozšířený ransomware, který se šíří zejména prostřednictvím emailů a infikovaných internetových odkazů. Poprvé se objevil v září 2013, jedná se tedy o **novou hrozbu**.

Krátce po nakažení v počítači **zašifruje veškerá dostupná uživatelská data** velmi silným kryptografickým nástrojem, který je v podstatě nemožné prolomit. Následně se objeví obrazovka požadující vysoké výkupné (obvykle ve výši kolem 300 amerických dolarů tj. zhruba 6000 korun) splatné ve virtuální měně bitcoin (případně jiným obtížně vystopovatelným platebním prostředkem) do 72 hodin. Odpočet nelze v tomto případě jednoduše zastavit ani změnou systémového času v biosu.

Pokud uživatel nezaplatí, červ se automaticky smaže včetně dešifrovacího klíče a data jsou tak nenávratně ztracena. Ani v případě zaslání platby není žádná záruka, že útočník své slovo splní – některým lidem po zaplacení klíč přišel, jiným nikoliv. Útočníci cílí hlavně na menší firmy, pro které je ztráta dat nenahraditelná a je vyšší pravděpodobnost, že výkupné zaplatí. Cryptolockerem se ale může nakazit kdokoliv, nejjistější ochranou je hlavně pravidelné zálohování dat, aktualizace bezpečnostního softwaru a opatrnost při otevírání neznámých souborů a internetových stránek. Pokud ale červ již uživatelská data zašifroval, pak je jejich dešifrování bez znalosti klíče i podle expertů nemožné. Podle ZDNet **je Cryptolocker jedním z nejúspěšnějších a nejsofistikovanějších virů současnosti** – jeho tvůrci již na výkupném vydělali podle odhadů přes 27 milionů dolarů (přes půl miliardy korun).

Tento virus je obdobou jiného známého ransomwaru tzv. policejního viru, o kterém jsme již informovali v jedné z minulých situačních zpráv, a který se bohužel v ČR šířil i ve druhé polovině roku 2013. Ten zablokuje uživateli přístup k počítači, zatímco na stránce se objeví loga českých bezpečnostních složek. Zobrazená zpráva říká, že zařízení bylo zablokováno policií z důvodu podezření na porušení zákona (ilegální stahování filmů, dětská pornografie atd.) a k jeho zpřístupnění je třeba zaplatit kauci. Není třeba dodávat, že tento virus nemá s Policií ČR vůbec nic společného, mnoho lidí ale raději výkupné zaplatí. Tzv. policejní virus je ovšem mnohem méně nebezpečný než Cryptolocker, protože počítač lze odborným zásahem opět odblokovat.

Vybrané události ve sledovaném období

Červenec

Sázková společnost Fortuna zažila rozsáhlé kybernetické útoky
Několik dní po sobě musela Fortuna čelit masivním systematickým útokům hackerů, které se projevily zhoršením dostupnosti jejích internetových stránek, zejména jejich výrazným zpomalením. Chodu sítě poboček se problémy nijak nedotkly. Společnost v této souvislosti podala trestní oznámení a útoky šetří policie.

Americká Sněmovna reprezentantů odmítla těsnou většinou omezení aktivit NSA
Americký protiteroristický program na tajné sledování internetu prošel první vážnou zkouškou na půdě Kongresu, když poslanci těsnou většinou odmítli pokusy omezit monitorování zákonem. Návrh na podvázání aktivit Národní agentury pro bezpečnost (NSA) odmítl poslanci Sněmovny reprezentantů těsným poměrem hlasů 217 ku 205.
Výkaz o hlasování potvrzuje, že citlivá otázka kontroly veřejných dat je problémem pro obě hlavní politické strany. Pro omezení činnosti NSA hlasovalo 94 republikánů, proti bylo 134, v demokratickém táboře byl poměr hlasů 111 ku 83. Důslednější kontrolu aktivit NSA prosazovala netradiční koalice republikánských konzervativců a demokratických liberálů. Předmětem hlasování byl takzvaný Amashův dodatek, který navrhl republikánský poslanec z Michiganu Justin Amash. Bezpečnostní služba měla podle návrhu mít právo například na monitorování internetu a telefonních hovorů jen v případě, že sledovaná osoba je vystavena policejnímu vyšetřování. NSA zároveň neměla dostat prostředky na sledování občanů USA ani na shromažďování osobních dat získaných z telefonní a e-mailové komunikace.

Podle průzkumu olomoucké univerzity se více než polovina dětí v ČR setkala s kyberšikanou
Alarmující výsledky přinesl průzkum připravený Pedagogickou fakultou Univerzity Palackého v Olomouci a společností Seznam.cz. Se šikanou vedenou prostřednictvím počítače, internetu, či mobilního telefonu, se podle něj setkalo 51% českých dětí. Nejčastější jsou verbální útoky, průniky na účet či obtěžování prozváněním. Asi 7% obětí kyberšikany se setkalo s vydíráním. U běžných forem kyberšikany přitom děti zpravidla nekontaktují dospělé. Průzkum byl velmi rozsáhlý – probíhal na více než 4000 školách a zúčastnilo se jej 21 tisíc dětí.

V USA se řešila jedna z největších hackerských kauz v dějinách
Prokuratura amerického státu New Jersey obvinila pětici cizinců ze zřízení rozsáhlé hackerské sítě, s jejíž pomocí připravili své oběti o stovky milionů dolarů. Obviněnými jsou čtyři Rusové a jeden Ukrajinec. K penězům se dostali přes krádeže kódů z kreditních karet, kterých získali nejméně 160 milionů. Podle agentury AP jde o největší hackerskou kauzu, jakou kdy americké soudy projednávaly. Mezi oběťmi jsou podle prokuratury například americká burzovní společnost Nasdaq, francouzský obchodní řetězec Carrefour, belgická banka Dexia a dalších zhruba deset velkých firem. Obvinění se nezákonnou činností podle vyšetřovatelů zabývali sedm let. Kódy z kreditních karet gang podle policie přeprodával do celého světa. Podle agentury Reuters byli obviněni Rusové Vladimir Drinkman, Alexandr Kalinin, Roman Kotov a Dmitrij Smiljaněc a Ukrajinec Mychajlo Ryti.

Srpen

Web New York Times napaden syrskými hackery

Internetová stránka významného amerického deníku The New York Times čelila v srpnu hned dvěma vlnám kybernetických útoků, které ji v obou případech na několik hodin vyřadily z provozu. Útok byl veden skupinou známou jako „Syrská elektronická armáda“, případně někým, kdo se za ni vydává. Syrská elektronická armáda se specializuje na DDoS útoky a defame internetových stránek Izraele, západních zemí a jejich spojenců. Ve svých prohlášeních obvykle podporuje režim Bašára Asada, třebaže není jasné, do jaké míry je s ním skutečně spjata. Její útoky trápí americká média pravidelně, obětí se v minulosti staly i Washington Post, časopis Time či televizní stanice CNN. Skupina často nahradí titulní stranu vlastním textem a obrázky, k DDoS útokům se obvykle přihlašuje na Twitteru. Koncem roku ovšem aktivity skupiny slábly, zřejmě v souvislosti s vývojem syrského konfliktu.

E-maily zneužívající Českou poštu byly součástí útoku ve 4 zemích

Nedávný e-mailový útok zneužívající Českou poštu byl součástí rozsáhlé kriminální akce ve čtyřech zemích. Zprávy vydávající se za sdělení renomovaných peněžních ústavů šířily virus, tzv. trojský kůň, odcizující osobní data. Uvedla to bezpečnostní skupina CSIRT.CZ. Podle některých zahraničních webů útok pochází z Česka.

Kampaň šířící škodlivý program pod názvem Hesperbot začala v České republice 8. srpna. Rozesílaná zpráva vypadala jako služba sledování balíku poskytovaná Českou poštou. Útočníci si za tímto účelem pořídili doménu ceskaposta.net, na kterou vedl skutečný odkaz z e-mailu. Ze stránky si uživatel nevědomky stáhl virus do počítače. Nový a velmi efektivní bankovní trojský kůň míří na uživatele v České republice, Portugalsku, Turecku a ve Velké Británii. Podle antivirové společnosti Eset má virus v Česku desítky obětí a došlo prý i k významným finančním ztrátám. Vedle České pošty se podvodný e-mail vydává například za zprávy od ČSOB, Komerční banky nebo Raiffeisen Bank. Cílem útočníků je získat přihlašovací údaje do bankovních účtů obětí a zároveň je donutit k instalaci dalšího viru na jejich telefon s platformou Android, Symbian, či Blackberry.

Hesperbot mimo jiné získává údaje o zmáčknutých klávesách na počítači, umí natáčet videa a pořizovat snímky obrazovky, sleduje také síťový provoz a dokáže ovládat napadený počítač na dálku. Podle dřívějšího vyjádření Jiřího Ptáčka ze společnosti NETservis jde o jeden z nejlépe provedených pokusů o získání citlivých dat z poslední doby.

Září

Nemocnice na Bulovce čelila hackerskému útoku

Ve čtvrtek 12. září zažila pražská nemocnice na Bulovce útok na svůj vnitřní informační systém, který musel být z bezpečnostních důvodů vypnut. Podle mluvčího nemocnice tak hackeři nepronikly k datům pacientů. Po dobu výpadku zajišťovala Bulovka nadále speciální lékařská vyšetření, běžné případy vozila záchranka po dohodě s dispečinkem rovnou do jiných nemocnic. Během dne se podařilo všechny systémy opět zprovoznit a obnovit normální provoz. Na odvrácení útoku nemocnice spolupracovala s Národním centrem kybernetické bezpečnosti a případ byl předán policii.

Němcům se podařilo během pár dnů prolomit zabezpečení nového iPhonu otiskem prstu

Jednou z hlavních novinek nového modelu iPhonu 5S od firmy Apple, který jej mělo odlišovat od konkurence, bylo průlomové zabezpečení přístroje snímačem otisků prstů. Byla dokonce vypsána odměna za jeho překonání. Jen pár dní po slavnostním představení nového přístroje přitom známá německá hackerská skupina Chaos Computing Club (CCC) zveřejnila video, na kterém se

jí podařilo odemknout přístroj pomocí vyfotografovaného otisku vytištěného na průsvitnou fólii. Otisk je přitom možné z displeje či tlačítka telefonu poměrně snadno sejmout (u dotykového displeje zanechávají uživatelé na přístroji otisků spousty). Jeden z hackerů, který video zveřejnil, uvedl, že otisk prstu by se neměl používat jako jediná forma zabezpečení, protože otisky zanecháváme téměř všude a není velký problém je okopírovat.

Říjen

Evropský měsíc kybernetické bezpečnosti

Dne 1. 10. 2013 odstartovala pod záštitou Mgr. Vladimíra Rohela, ředitele Národního centra kybernetické bezpečnosti, kampaň Evropský měsíc kybernetické bezpečnosti. Pro území České republiky ji organizuje Národní centrum bezpečnějšího internetu. Hlavními cíli kampaně bylo prohloubit komunikaci a spolupráci mezi státními institucemi, neziskovými organizacemi, a komerčními společnostmi, které se podílejí na vytváření bezpečnějšího online prostředí.
Projekt Evropský měsíc kybernetické bezpečnosti podporuje Evropská agentura kybernetické bezpečnosti (ENISA) společně s místopředsedkyní Evropské Komise a komisařkou zodpovědnou za digitální agendu Neelie Kroes. Akce zahrnuje na padesát různých aktivit a spolupráci více než čtyřiceti soukromých i veřejných subjektů v pětadvaceti zemích Evropské Unie.

Uzavření online tržiště Silk Road, zneužívaného k trestné činnosti, včetně prodeje drog

Americký FBI zatkl v San Franciscu 29letého tvůrce a vlastníka známého internetového tržiště Silk Road (Hedvábná stezka) Williama Ulbrichta. Zároveň byla při zásahu zabavena virtuální měna bitcoin v hodnotě 3,6 milionu dolarů (asi 68 milionů korun).
Silk Road umožňoval prodejcům i nakupujícím přísnou anonymitu díky používání systému Tor, maskujícího IP adresy. Velmi si ho proto oblíbili zejména drogový dealeři, podle amerických policistů se přes něj prodalo několik set kilogramů narkotik. Nabídku k zakoupení kvalitního heroinu či kokainu využívali údajně i čeští uživatelé, kterým zásilka obvykle dorazila obyčejnou poštou. Platilo se přitom výhradně těžko vystopovatelnou virtuální měnou. Ze Silk Road se tak postupně stal zřejmě nejrozsáhlejší kriminální trh na internetu, kde bylo možné kromě drog sehnat i zbraně či si objednat nájemného vraha. Portál byl součástí tzv. hlubokého webu, který běžné vyhledavače neindexují.
Ulbricht byl obviněn ze spiknutí k obchodování s drogami, hackerství a ze spiknutí k praní špinavých peněz. Prozradila ho přitom poměrně triviální chyba, kdy se na odborných technických stránkách ptal vlastním jménem na specifický kód pro skryté internetové stránky, který později použil právě při tvorbě Hedvábné stezky. Na základě podobných stop je v současné době některými uživateli internetu podezírán Čech z vytvoření a následného „vytunelování“ online tržiště Sheep Marketplace, který byl označován za nástupce Silk Road (více viz zprávy za prosinec).

Policie ČR dopadla tři cizince podezřelé z počítačového pirátství

Plzeňským kriminalistům se podařilo dopadnout trojici mužů, kterým se podařilo podvodným způsobem získat z účtu jedné firmy na Plzeňsku téměř dva miliony korun. Útok byl veden pomocí phishingu: tentokrát šlo o email, který se vydával za informace od České pošty. Cizince zatkla zásahová jednotka v Hradci Králové, když se pokusili ukradené peníze vybrat z předem založených účtů. Je pravděpodobné, že byli součástí organizované skupiny. Dva zadržení byli obviněni z podílnictví a jeden z nich skončil ve vazební věznici.

Útoky Anonymous v Austrálii a na Filipínách

Indonéští hackeři, hlásící se ke skupině Anonymous, napadli několik desítek australských internetových stránek. Útok byl podle všeho reakcí na zprávy o australském podílu na špehování indonéských uživatelů americkou NSA, které vynesl Edward Snowden. Na postižených stránkách se totiž objevil nápis „Přestaňte špehovat Indonésii“. Napadené weby patřily ovšem z větší části

mezi „snadné“ cíle, protože se jednalo především o stránky drobných podnikatelů. Indonésie patří mezi hlavní zájmové oblasti australských zpravodajských služeb, protože se jedná o vůbec nejlidnatější zemi, ve které dominuje islám, a která se rozkládá velmi blízko od australských břehů. Přibližně ve stejné době čelili útokům Anonymous také Filipíny a Singapur.

Íránští hackeři pronikli do sítě amerického námořnictva

Úspěšný průnik do intranetu Navy Marine Corps (NMCI) se v září podle agentury AP podařil hackerům napojeným na Írán. NMCI patří mezi nejrozsáhlejší počítačové sítě na světě, odhadem je do ní připojeno přes 350 tisíc zařízení v USA a v Japonsku. Íránci údajně pronikli jen do té části sítě, která neobsahuje žádné utajované či citlivé informace. Přesto se jedná o další potvrzení četnosti kybernetických incidentů, jejichž původ lze v Íránu vysledovat. Nejčastějším cílem jsou pak americké firmy, zejména ty působící v energetickém sektoru.

Listopad

Odhalena krádež dvou milionů hesel pomocí botnetu

Firmě TrustWare se podařilo během listopadu odhalit a vystopovat botnet s názvem Ponny, který byl provozován ze serveru v Nizozemsku. Útočníkům se podařilo jeho prostřednictvím ukrást obrovské množství hesel do několika tisíc internetových služeb, nejvíce byl zastoupen Facebook (318 tisíc kompromitovaných účtů), služby Google (Gmail, Google+, YouTube; asi 70 tisíc účtů) a Twitter (22 tisíc účtů). Do Nizozemska odesílal tyto údaje virus integrovaným systémem keylogger, který zaznamenává stisknuté klávesy.

Napadena byla zařízení v zemích celého světa, je velmi pravděpodobné, že mezi nimi byla i Česká republika. Při analýze ukradených hesel se opět potvrdilo, že uživatelé nepřistupují k jejich tvorbě příliš zodpovědně – velké množství z nich mělo snadno zneužitelnou podobu (nejčastěji „123456“ či prosté „password“).

Krátce po udělení vysoké pokuty skončil server Hotfile. Všichni uživatelé přišli o svá data.

Nedlouho po uzavření portálu Megaupload byla ve spojených státech uzavřena další široce využívaná služba, určená pro ukládání dat – server Hotfile.com. Také v tomto případě byly důvodem spory o autorská práva, zde pak konkrétně soudní proces s Americkou filmovou asociací. Ten sice nakonec skončil dohodou o vyrovnání ve výši zhruba 1,6 miliardy korun a dohodou o zavedení filtrovacích mechanismů pro odstraňování pirátských kopií, provozovatelé služby se ale nakonec rozhodli provoz bez varování zcela ukončit. O uložená data tak přišli všichni uživatelé, tedy nejen počítačoví piráti, ale i řada jednotlivců a firem, kteří server využívali jako levné úložiště. Některé menší firmy sem dokonce ve snaze ušetřit přesunuly většinu svých interních dat a náhlé uzavření serveru jim způsobilo nemalé problémy.

Na zmíněné stránce tak lze nyní nalézt pouze zprávu o rozhodnutí soudu a upozornění, že existuje velké množství online platforem, kde lze filmy i seriály stahovat legální cestou.

Muži z jižní Moravy hrozí za sdílení filmů až 8 let vězení a náhrada škody ve výši 28 milionů

V listopadu provedla Policie České republiky domovní prohlídku u 37letého muže z Blanska, po které mu bylo sděleno obvinění ze spáchání trestného činu porušení autorského práva. Muž, který na síti vystupoval pod přezdívkou Icathan, patřil mezi nejaktivnější počítačové „piráty“, když na internetu nasdílel téměř čtyři stovky filmů a hudebních alb. Distributoři a vlastníci autorských práv již škodu předběžně vyčíslili na 28 milionů Kč, kterou budou na obviněném vymáhat. Zároveň mu za jeho činnost hrozí až 8 let vězení, a to i přesto, že ze své činnosti nikterak výrazně neprofitoval.

Deník Právo v souvislosti s případem zveřejnil vyjádření zástupce ředitele blanenské a vyškovské policie Zdeněk Grénar, který řekl: „obyčejný člověk takovou škodu, jaká byla vyčíslena v tomto případě, nemůže do smrti nikdy splatit. Spousta lidí si ani neuvědomuje rizika, která hrozí, když

například nechají stáhnout kamarádovi nějaký film. Škoda se v takových případech vyčísluje podle ceny originálního nosiče, a proto se pak dostáváme do tak vysokých čísel.“ Podnět k vyšetřování podala Česká protipirátská unie a policie je v takovém případě povinna konat. Nelegální sdílení filmů či hudby tak může vést k poměrně závažným koncům a lze očekávat, že podobných případů bude v České republice přibývat.

Rádio Svobodná Evropa čelilo útoku hackerů
Americká rozhlasová stanice Rádio Svobodná Evropa/Rádio Svoboda se stala v listopadu terčem DDoS útoku, při kterém bylo narušeno její internetové vysílání a přístup na webové stránky. Dosud není jasné, kdo za útokem stál. Svobodná Evropa se zaměřuje zejména na vysílání do zemí, jako je Írán, Pákistán, či Rusko, kde podle jejích provozovatelů panuje cenzura či neexistuje svobodný přístup k informacím.

Český vládní CERT byl zařazen na seznam evropského sdružení Trusted Introducer
Vládní CERT (GovCERT.CZ) byl k 19. listopadu 2013 zařazen na seznam Terena-Trusted Introducer. Sdružení Trusted Introducer (TI) působí v rámci evropské organizace TERENA a sdružuje evropské bezpečnostní týmy vládní, národní, komerční sféry (např. bank, provozovatelů internetového připojení, výrobců hardware ad.) nebo univerzit. Z České republiky jsou k dnešnímu dni členy TI tyto týmy: Vládní GovCERT.CZ, Národní CSIRT.CZ, ACTIVE24-CSIRT, CESNET-CERTS, CSIRT-MU, CZ.NIC-CSIRT a SEZNAM.CZ-CSIRT.
Provozovatelem vládního bezpečnostního týmu GovCERT.CZ je Národní bezpečnostní úřad (NBÚ) prostřednictvím své organizační složky, Národního centra kybernetické bezpečnosti (NCKB). Úlohou NCKB je koordinace spolupráce na národní i mezinárodní úrovni při předcházení a řešení incidentů a kybernetických útoků.
GovCERT.CZ zahájil proces registrace v říjnu 2013. Vstup Vládního CERT České republiky mezi registrované týmy TI znamená další krok k užší spolupráci se světovou infrastrukturou bezpečnostních týmů CERT nebo CSIRT a zvýšení prestiže na mezinárodní scéně. GovCERT.CZ začátkem příštího roku podá žádost o vyšší stupeň spolupráce, tzv. akreditaci. Jedná se o placené členství, z něhož mj. vyplývá přístup k celé řadě informací a kontaktů v partnerských evropských zemích.

Prosinec

Čínským hackerům se podařilo napadnout počítače ministerstev pěti evropských zemí, údajně včetně ČR
Proniknout do vnitřních sítí ministerstev zahraničí Portugalska, Lotyšska, Bulharska, Maďarska a České republiky se údajně podařilo čínským hackerům v průběhu summitu G20 v Petrohradě. Útok byl veden klasickou metodou phishingu, kdy byli zaměstnancům úřadů zasílány emaily z neznámých adres, jejichž předmět sliboval informace o konfliktu v Sýrii (toto téma summitu dominovalo), případně dokonce fotky nahé manželky francouzského exprezidenta Sarkozyho Carly Bruniové. Úředníci, kteří zavirované přílohy otevřeli, stáhli do vnitřní sítě zároveň čínský spyware. Zprávu přinesl v prosinci deník New York Times s odvoláním na bezpečnostní experty. Není ovšem jasné, zda se jednalo o útok iniciovaný přímo čínskou vládou, ani zda došlo k úniku konkrétních informací. Ministerstvo zahraničí České republiky informace o útoku oficiálně nepotvrdilo.

Z internetového tržiště zmizelo 800 milionů Kč. Stopy obřího podvodu vedou do ČR.
Internetové tržiště Sheep Marketplace přerušilo na přelomu listopadu a prosince nečekaně svůj provoz. Jeho administrátoři nejprve zveřejnili zprávu o tom, že se portál stal terčem hackerského útoku, následně ho ale bez varování uzavřeli a zcela přestali komunikovat. V jejich držení tak podle časopisu Forbes zřejmě zůstává zhruba 40 milionů dolarů (800 milionů korun) ve virtuální měně bitcoin. Podle některých zdrojů mohlo být Sheep Marketplace řízeno z České republiky, identita jeho tvůrců ale zůstává nejasná.

První nitky vedou k českému programátorovi, který před časem na českých i zahraničních fórech hledal rady ohledně provozování skrytého online tržiště. Ten ale své zapojení do projektu důrazně odmítá, bránit se hodlá i právní cestou. Vypátrali ho sami uživatelé internetu, přičemž někteří z nich po něm již požadují navrácení ukradených peněz, a dokonce mu vyhrožují fyzickou likvidací (mezi obětmi podvodu je řada zločinců, zejména z řad distributorů drog). Stejným způsobem byl odhalen a následně zatčen tvůrce portálu Silk Road (Hedvábná stezka) William Ulbricht. Okolnostem konce Silk Road se blíže věnuje část „Uzavření online tržiště Silk Road, masově zneužívaného k trestné činnosti, včetně prodeje drog“ na straně 64 této zprávy (sekce říjen).

Spolupráce FBI, Europolu a Microsoftu pomohla zlikvidovat jeden z největších botnetů současnosti

Botnet ZeroAccess, který až do prosince ovládal odhadem 1,9 milionu počítačů v mnoha zemích světa, se podařilo zlikvidovat díky mezinárodní spolupráci. ZeroAccess využíval této rozsáhlé sítě zombie zařízení infikovaných malwarem, aby jim vkládal do prohlížečů falešné výsledky vyhledávání. Kdo takový odkaz otevřel, byl přesměrován na stránky se zobrazovanou reklamou. Právě z vysokého počtu přístupů na stránky s reklamou inkasovali tvůrci peníze, neboť z každého zobrazení měli provizi. Celkem si tak mohli přijít až na 2,7 milionu dolarů (cca 54 milionů korun) měsíčně. Krom toho byl botnet ZeroAccess podle všeho zneužíván i k DDoS útokům.

Americký federální soud pak na základě žaloby umožnil blokovat komunikaci mezi napadenými počítači v USA a doménami, které botnet využíval. Ve spolupráci s místními úřady pak Europol inicioval provedení domovních prohlídek v několika evropských zemích (Německo, Švýcarsko, Nizozemsko, Lucembursko a Lotyšsko) během kterých byly zabaveny počítače spojené s provozováním ZeroAccess.

Jednání zástupců středoevropských CERT/CSIRT týmů v Praze

Ve dnech 18. - 19. 12. 2013 proběhlo druhé setkání skupiny zástupců CERT a CSIRT týmů středoevropského regionu „Central European Cyber Security Platform“ (CECSP) v Praze. Platforma sdružuje vládní a národní týmy České Republiky, Maďarska, Polska, Rakouska a Slovenska zabývající se kybernetickou bezpečností.

Platforma byla založena v květnu 2013 z iniciativy rakouského vládního CERT a Národního centra kybernetické bezpečnosti (NCKB), které je organizační složkou Národního bezpečnostního úřadu (NBÚ). NCKB kromě jiného plní i roli Vládního CERT České republiky. První setkání CECSP proběhlo v České republice na půdě NBÚ a jeho hlavním cílem bylo založení platformy a stanovení cílů a strategií. Druhé, prosincové setkání platformy bylo věnováno technickým věcem v oblasti kybernetické bezpečnosti. Po prvním jednání se účastníkům tato iniciativa jevila jako potřebná a užitečná. Po druhém se všichni zástupci shodli na jejím významu a přínosu pro spolupráci v regionu. I proto podpořili myšlenku jejího dalšího pokračování. CECSP do 19. prosince předsedala Česká republika prostřednictvím NBÚ, po Česku převzalo předsednictví pro rok 2014 Rakousko a další jednání bylo naplánováno na konec dubna 2014 ve Vídni.

Účastníci druhého setkání v prezentacích popsali svá technická řešení a představili zajímavé mezinárodní projekty v oblasti kybernetické bezpečnosti. V diskusích se probíraly možnosti sdílení informací, datových zdrojů pro aplikace i zkušeností, proběhla různá jednání a byly navázány dvou i vícestranné spolupráce.

Zástupce NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) detailně představil letos proběhlé cvičení v oblasti kybernetické bezpečnosti „Locked Shields“, zejména jeho technické pozadí a možnosti. Zástupkyně evropské agentury ENISA (European Union Agency for Network and Information Security) představila jejich činnosti v oblasti metodické podpory CERT/CSIRT týmům, školení, cvičení a poukázala na jejich publikační činnost, která je volně dostupná ke stažení na stránkách agentury.

V diskusi byla také řešena témata společné platformy pro sdílení informací o malware (MISP), společných cvičení, mezinárodní sdílení dat k incidentům a návrhu společné deklarace, která by měla nyní projít připomínkami členů a být schválena na dalším jednání.
Bylo otevřeno téma jednání skupiny Central European Policy Institute (CEPI) na Cyber Visegrad Workshop, které proběhlo paralelně 18. prosince 2013 v Bratislavě a na které zástupci CECSP okamžitě reagovali písemným prohlášením, které bylo 19. prosince odpoledne zasláno CEPI, viz níže. Jednání ukončil ředitel NBÚ Dušan Navrátil předáním pomyslného předsednického žezla ve formě dřevěné paličky s podstavcem zástupci rakouské strany.

Zdroje pro tuto kapitolu: cleverandsmart.cz, PČR, ČTK, sxc.hu, idnes.cz, europol.europa.eu,aphaia.co.uk, allpremium4.blogspot.com, aktualne.centrum.cz, govcert.cz, lidovky.cz, novinky.cz, technet.idnes.cz, zive.cz, e15.cz, trustport.com, csas.cz, kickstarter.com, interpol.int, hpsolutions.cz, economist.com, csoonline.com, edition.cnn.com, enisa.europa.eu, en.wikipedia.org, tomshardware.com, stanford.edu, chip.cz, newscientist.com, russelwebster.com, eset.cz, businessworld.cz, itbiz.cz, infoworld.com, europa.eu computerworld.cz, net-security.org, mcafee.com, itnewsafrica.com, scmagazine.com.au, businessinsider.com, blackhat.com,

KRIZOVÉ ŘÍZENÍ

Hasičské statistiky a jejich interpretace

Namísto policejních statistik se v tomto případě soustředíme na statistiky Generálního ředitelství Hasičského záchranného sboru ČR, konkrétně na data z období 1.1. – 30.9. 2013 (údaje z posledního čtvrtletí se dosud zpracovávají). Tyto statistické výstupy jsou v podrobnější verzi pravidelně aktualizovány rovněž na stránkách www.hzscr.cz.

V období od 1. ledna do 30. září 2013 zasahovaly jednotky požární ochrany u **88 750 událostí,** což je o **9,7%** více než ve stejném období roku 2012. Nejčetnějšími událostmi byly **technické havárie – 58,8%, následují dopravní nehody – 15,7%, požáry – 14,1%, úniky nebezpečných chemických látek – 4,6%. Plané poplachy činí 6,8 % z celkového počtu událostí. Nejvíce událostí bylo v červnu** – 21,1% z celkového počtu, nejméně v únoru – 7,0%. Podle dnů v týdnu bylo **nejvíce** událostí v **neděli** – 16,9% a **nejméně** v sobotu – 12,3%.

1. Počet událostí se zásahem jednotek PO

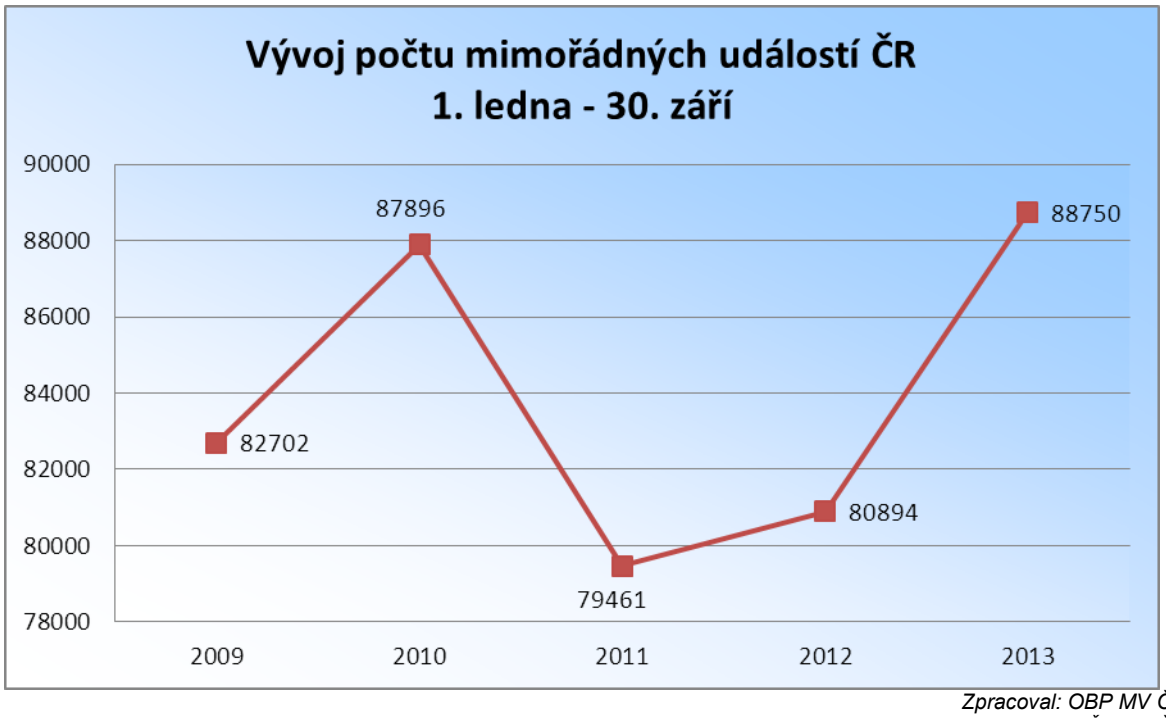
Druh události	2011	2012	2013	Index
Požáry s účastí jednotky PO	16 030	16 355	12 532	77
Dopravní nehody	12 214	13 757	13 937	101
Úniky nebezpečných látek	4 142	3 890	4 066	105
z toho „ropných produktů“	3 313	3 046	3 187	105
Technické havárie	40 771	40 666	52 201	128
Radiační havárie a nehody	1	1	0	0
Ostatní mimořádné události	7	39	19	49
Plané poplachy	6 296	6 186	5 995	97
UDÁLOSTI CELKEM	79 461	80 894	88 750	110

Zdroj: MV-GŘ HZS ČR

Pokud se podíváme na rozložení mimořádných událostí v rámci ČR, pak na jejich počet jednoznačně vedou kraje Moravskoslezský a Středočeský. Celá třetina mimořádných událostí ve sledovaném období se odehrála v těchto dvou krajích. Střední Čechy navíc v prvních třech čtvrtletích roku 2013 vůbec poprvé po mnoha letech vystřídaly severní Moravu a obsadily nechtěné první místo jako kraj s největším počtem hasičských výjezdů (12 896). Došlo zde také k vůbec největšímu nárůstu, kdy se počet mimořádných událostí zvýšil téměř o třetinu (zatímco v Moravskoslezském kraji ve srovnání se stejným obdobím roku 2012 o 8% klesl na 12 583).

Pohoršily si bohužel všechny kraje s výjimkou Královéhradeckého, Pardubického, Olomouckého a právě Moravskoslezského. Průběžná čísla nasvědčují tomu, že v přepočtu na počet obyvatel zůstane Vysočina nelichotivým premiantem v počtu mimořádných událostí. V roce 2012 si naopak v tomto směru vůbec nejlépe vedl kraj Zlínský.

Počet mimořádných událostí v ČR má bohužel po dramatickém poklesu v roce 2011 opět stoupající tendenci, jak přehledně znázorňuje následující graf:



Zpracoval: OBP MV ČR
Zdroj dat: MV-GŘ HZS ČR

Počet **dopravních nehod,** jejichž následky likvidovaly jednotky PO, letos vzrostl o 1 %. Nejčetnější byly zásahy u dopravních nehod ve Středočeském kraji – 2 207 (- 20), minimum bylo v kraji Karlovarském – 394 (+7). Celkově u nehod hasiči bezprostředně zachránili či evakuovali 4 414 osob (- 1 485), při zásazích se vyskytlo také 461 usmrcených osob (-26) a 9 904 zraněných osob (+110), jimž v mnoha případech poskytli předlékařskou pomoc.

Z **úniků nebezpečných chemických látek** byly nejčetnější úniky ropných látek – 3 187 (+141), úniky plynů a aerosolů – 557 (+49), kapalin mimo ropných produktů – 236 (-32), dále pevných látek – 5 (-6) a ostatních včetně potravinářských produktů – 81 (+24). Nejvyšší počet těchto případů byl ve Středočeském kraji – 612 (+32), nejnižší v kraji Pardubickém – 32 (+1).

Kategorie **technické havárie** zahrnuje technické havárie – 8 (-3), technické pomoci – 47 104 (+10 288), technologické pomoci – 693 (+180) a ostatní pomoci – 4 396 (+1 070). 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 – 8 330 (-35), nejméně ve Zlínském kraji – 1 302 (-57). **Ostatní mimořádné události** zahrnují zejména zásahy spojené s plněním mimořádných úkolů při řešení „AKCE METANOL“ v České republice.

Plané poplachy oproti stejnému období roku 2012 o 3 % poklesly, přičemž jejich podíl na celkovém počtu událostí také poklesl a činí 6,8 %. Nejčetnější jsou plané poplachy způsobené elektrickou požární signalizací (46,7 %), další plané poplachy jsou způsobeny přivoláním k případu, který měl příznak požáru (19,7 %), zneužití jednotky PO (5,2 %), přivolání k nenahlášenému pálení (9,4 %) a z jiných důvodů (19 %). Nejvíce planých poplachů bylo v hl. m. Praze – 966 (+88), nejméně v kraji Libereckém – 185 (+16).

Jednotky PO bezprostředně zachránily nebo evakuovaly z ohrožených prostor za období leden – září letošního roku **33 858** (-25 053) osob - nejvíce při technických pomocích, požárech, dopravních nehodách. Zároveň bylo **344** hasičů zraněno (-21), z toho 244 profesionálních (-21) a 100 dobrovolných (0).

Při zásazích se vyskytlo také **1 598** (-685) usmrcených osob - jednotky PO pomáhaly při jejich vyprošťování a vynášení při dopravních nehodách, požárech a při nouzovém otevírání bytů. Dále byla **14 486** (+717) zraněným osobám poskytnuta předlékařská pomoc (převážně u dopravních nehod, technických pomocí a požárů).

V období od 1. ledna do 30. září 2013 vzniklo v ČR **12 934** požárů s účastí i bez účasti jednotek PO (-3 859). Přímé škody dosáhly částky **1 877,3 mil. Kč** (-122,6). Při požárech bylo **80 osob usmrceno** (-21) a dalších **851 osob bylo zraněno** (-111). Jednotky PO uchránily před zničením hodnoty ve výši **10,7 mld. Kč** (+2,5). Počet požárů je oproti stejnému období roku 2012 nižší o 23 %, přímé škody jsou nižší o 6,1 %, počet usmrcených je nižší o 20,8 %, počet zraněných nižší o 11,5 %. Nejvíce požárů vzniklo v červenci – 15,8 % z celkového počtu, nejméně naopak v únoru – 7,8 %. Podle dnů v týdnu hořelo nejčastěji v neděli – 15,3 % a nejméně ve středu – 13,3 %.

Požáry - základní ukazatele v období leden - září

Rok	Počet požárů	Škoda mil. Kč	U	Z
2011	16 499	1 806,5	94	826
2012	16 793	1 999,9	101	962
2013	12 934	1 877,3	80	851

U - počet usmrcených osob, Z - počet zraněných osob

Zdroj: MV-GŘ HZS ČR

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

1. čtvrtletí

9. 1. – **Sklad elektroniky v budově průmyslového areálu bývalého podniku SVIT** (poškozeno více firem), Zlín.
Příčina: vznícení hořlavin od zářivkového tělesa.
Škoda: 398 551 000 Kč.
Zraněny: 4 osoby.

2. čtvrtletí

29. 4. – **Čtyřpodlažní dům,** Praha 1 – Divadelní ulice.
Příčina: výbuch plynu po úniku z plynového řádu.
Škoda: 100 000 000 Kč.
Zraněno: 43 osob. Zachráněny: 2 osoby. Evakuováno: 230 osob.

16. 5. – **Sklad ratanového nábytku firmy FAKOPA spol. s.r.o.**, Děčín.
Příčina: v šetření.
Škoda: 30 000 000 Kč.
Zraněni: 3 hasiči. Evakuováno: 200 osob.

26. 5. – **Sklad píce firmy ZEMO – PROFIT a.s.**, Mnich, okr. Pelhřimov.
Příčina: úmyslné zapálení.
Škoda: 22 330 000 Kč.

3. 6. – **Výrobní hala firmy KOVOLIS HEDVIKOV a.s.**, Ronov nad Doubravou, okr. Chrudim.
Příčina: v šetření.
Škoda: 50 000 000 Kč.
Zraněna: 1 osoba.

2. čtvrtletí – 2. část

10. 6. – **Trafostanice firmy TŽ a.s.**, Třinec, okr. Frýdek – Místek.
Příčina: technická závada – elektrický zkrat na odpojovači fáze.
Škoda: 22 000 000 Kč.

18. 6. – **Trafostanice firmy ČEPS a.s.**, Praha – Šeberov.
Příčina: technická závada.
Škoda: 100 000 000 Kč.

3. čtvrtletí

11. 7. – **Budova penzionu a restaurace**, Velký Ratmírov u Jindřichova Hradce
Příčina: úder blesku.
Škoda: 30 000 000 Kč.

30. 7. – **Strojovna bioplynové stanice ZD CHOVATELŮ A PĚSTITELŮ**, Litomyšl, okr. Svitavy.
Příčina: úder blesku a vznícení kabelového vedení.
Škoda: 25 000 000 Kč.

31. 7. – **Velkokapacitní seník s fotovoltaickými panely firmy AGRA Řisuty spol. s.r.o.**,
Malíkovice – Čanovice, okr. Kladno.
Příčina: nedbalost při svařování hydroizolační lepenky.
Škoda: 20 000 000 Kč.
Zraněni: 2 hasiči.

Přehled připravovaných velkých cvičení pro rok 2014

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: 11. – 12. listopadu 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.

BLACKOUT 2014
- Cvičení akceschopnosti a reakce vybraných úřadů a složek IZS na rozsáhlý výpadek elektřiny v hlavním městě.
- Termín provedení: 1. čtvrtletí 2014

NÁKAZA 2014
- Součinností veterinární cvičení, likvidace nebezpečné nákazy zvířat. Organizátorem je Ministerstvo zemědělství ČR.
- Předpokládaná doba a místo konání: 16. – 19. června 2014; vojenský újezd Květušín, Boletice

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

Exkurz:
Problematika aktivního střelce v ČR

Fenomén aktivního střelce je v posledních 20 letech stále aktuálnějším tématem. Ačkoli bylo nejvíce případů zaznamenáno v USA, své zkušenosti již mají také evropské státy. Bezpečnostní složky ČR nemají se zákrokem proti typickému případu aktivního střelce příliš zkušeností. Na území ČR došlo k několika případům, které vykazují podobné znaky chování takovýchto pachatelů, tzn., že cílem jejich jednání je zranit či zabít co nejvíce osob, postupovat systematicky a podle předem promyšleného plánu a zpravidla nevyjednávat s policií. Mezi mediálně známé případy patří bezesporu ten z roku 2005, kdy osmadvacetiletý muž náhodně a v relativně krátkém časovém sledu na území ČR zabil 3 osoby. Dalším takovým případem může být útok šestadvacetiletého muže, ke kterému došlo v červnu roku 2011, při útoku nedošlo ke ztrátám na životech a zraněny byly 3 osoby.

Chování aktivního střelce není podmíněno vždy použitím střelné zbraně. Tento aspekt je dán možností pachatele dostat se ke střelné zbrani a použitelné munici. Na území ČR byly v posledních letech zaznamenány i případy, kdy k podobnému typu útoku byly využity chladné zbraně nebo výbušné předměty. Za útok aktivního střelce či útočníka lze považovat také čin Olgy Hepnarové z července roku 1977, která nákladním automobilem Praga RN zabila 8 lidí a 17 zranila.

Problematikou aktivního střelce a jeho eliminace se v roce 2013 intenzivně zabývaly také bezpečnostní složky v ČR. V průběhu roku 2013 proběhla v jednotlivých krajích cvičení zaměřená na eliminaci aktivního střelce a zvýšení připravenosti bezpečnostních a záchranných složek. Cvičení byla realizována z pokynu náměstka policejního prezidenta pro vnější službu z ledna roku 2013. Při cvičeních nebyl pevně stanoven scénář, jednotícím prvkem byl pouze zásah v prostředí školy. Záleželo také na jednotlivých krajských policejních ředitelstvích, zda bude cvičení realizováno v součinnosti s ostatními složkami integrovaného záchranného systému, či zda bude prověřen pouze taktický zásah Policie ČR. Cílem cvičení bylo prověření připravenosti bezpečnostních a záchranných složek na situaci aktivního střelce v budově školy.

Výjimku ve scénáři realizovaných cvičení pak tvořilo cvičení ve stanici metra Florenc v Praze, které proběhlo v červnu. Přestupní stanice byla zvolena záměrně kvůli své rozsáhlosti a z ní vyplývající obtížnosti a složitosti zákroku bezpečnostních a záchranných složek. Cvičení v podobném duchu by měla být realizována také v roce 2014.

Exkurz:
Cvičení Blaník 2013

Vnitrostátní cvičení s názvem „BLANÍK 2013“ proběhlo na několika místech České republiky, zejména v Praze a Karlových Varech, ve dnech 27. – 29. 11. 2013.

Cvičení bylo zacíleno na činnost ústředních správních úřadů, zpravodajských služeb, Policie ČR, složek Integrovaného záchranného systému a dalších subjektů. Za tímto účelem byla vytvořena fiktivní situace ohrožení obyvatel ČR teroristickým útokem.

Cílem cvičení bylo především:

- zdokonalit činnost krizových štábů,
- procvičit efektivitu postupů v oblasti boje proti terorismu, zajišťování veřejného pořádku a ochrany civilního letectví,
- prověřit reálnost zpracovaných krizových, typových a operačních plánů.

Pro potřeby cvičení byla simulována situace, kdy několik ozbrojenců z fiktivní teroristické organizace vtrhlo do odletové haly mezinárodního letiště Karlovy Vary, kde zadrželo cca dvě desítky rukojmích a požadovalo mimo jiné přistavení letadla a bezpečný odlet. Vzhledem k vážnosti situace bylo nutné svolat Ústřední krizový štáb, který vedl ministr vnitra Martin Pecina a první náměstek pro vnitřní bezpečnost Lubomír Metnar.

Jen z řad Policie České republiky se cvičení zúčastnilo na 160 příslušníků a zaměstnanců. Zapojenými útvary byly především Krajské ředitelství policie Karlovarského kraje, Útvar rychlého nasazení, Útvar pro odhalování organizovaného zločinu SKPV, Krajské ředitelství policie Plzeňského kraje a další útvary z řad Policejního prezidia ČR, především příslušníci spadající pod úsek vnější služby.

Po obsazení letiště teroristy, zajistili policisté bezpečnostní perimetr, zejména s ohledem na zajištění bezpečnosti dalších osob. Následovala intenzivní policejní činnost spočívající mimo jiné v získávání a vyhodnocování informací a následném vyjednávání s teroristy. Ti během cvičení vznášeli různé požadavky, na které musel velitel opatření adekvátně reagovat. Vyhověním některým z nich bylo například dosaženo propuštění části rukojmích.

V odpoledních hodinách přišel požadavek na přistavení letadla a volný odlet. Dříve, než se o případném splnění tohoto zásadního požadavku mohlo rozhodnout, bylo paralelně zasedajícím Ústředním krizovým štábem doporučeno silové řešení situace, které na místě provedli příslušníci Útvaru rychlého nasazení. Jeho výsledkem byla eliminace teroristů a osvobození rukojmích.

Z celého cvičení byla pořízena velmi rozsáhlá fotografická a video dokumentace. Takto získané materiály budou následně podrobně analyzovány a výstupy z nich použity pro další zkvalitnění taktických postupů Policie České republiky při mimořádných událostech spojených s terorismem a ohrožením civilního leteckého provozu.

Kromě reálného nácviku zainteresovaných policejních útvarů, se cvičení účastnilo i několik dalších složek Integrovaného záchranného systému. Cvičení bylo ukončeno dne 29. listopadu 2013 v 15 hodin.

Po cvičení bude následovat vyhodnocení, jehož cílem bude analyzovat postupy zúčastněných orgánů a navrhnout zlepšení v případě, že budou zjištěny nedostatky. Cvičení orgánů krizového řízení, tedy prověřování připravenosti složek Integrovaného záchranného systému na zvládání možných krizových situací, vyplývá z „Plánu cvičení orgánů krizového řízení – upřesnění na léta 2013–2015“, schváleného Bezpečnostní radou státu.

Exkurz: Vyhodnocení povodní 2013

V červnu loňského roku zasáhly rozsáhlé území České republiky povodně. Po jejich odeznění vydala vláda ČR usnesení ze dne 3. července 2013 č. 533 k realizaci projektu Vyhodnocení povodně v červnu 2013.

Tento projekt je rozdělen do 4 tematických oblastí a 13 dílčích úkolů a předmětem vyhodnocení jsou všechny aspekty povodňové situace, jejích příčin, průběhu, provedených opatření a jejich účinnosti, sociálních, zdravotních a ekonomických důsledků. Postupně jsou zpracovávány dílčí zprávy (např. Předběžná zpráva projektu Vyhodnocení povodní v červnu 2013) a celý projekt bude zakončen souhrnnou závěrečnou zprávou v červnu 2014, která bude obsahovat závěry a návrhy opatření z jednotlivých oblastí.

Na základě výše uvedeného usnesení vlády bude také posouzena stávající právní úprava řízení krizových situací za povodní na národní úrovni a kompetence Ústředního krizového štábu a Ústřední povodňové komise podle zákona č. 240/2000 Sb., krizový zákon a zákona č. 254/2001 Sb., vodní zákon. Za tímto účelem bude ustavena odborná pracovní skupina, která bude mít za úkol analyzovat stávající stav a navrhnout možná řešení vzniklé situace.

Vybrané události ve sledovaném období

Srpen

Kynologové cvičili nejen sutinové vyhledávání
V dnech 29. – 31. srpna 2013 se v Kaznějově a okolí konala odborná příprava atestovaných kynologů ve specializaci sutinové vyhledávání. Instrukčně metodické zaměstnání organizuje MV-generální ředitelství HZS ČR a bylo zaměřeno na sutinové vyhledání zavalených osob ve zřícených objektech a následné záchranné práce, pohyb a práci psovoda se psem na místě zásahu a spolupráci s USAR odřadem Praha na místě zásahu. Součástí výcviku byla i práce a činnost psovoda se psem na vodním toku řeky Berounky. Výcvik simuloval reálné podmínky nasazení kynologů a záchranářských psů např. na mezinárodní zahraniční operaci a tomu budou přizpůsobeny i náměty scénářů a připravené pracoviště v místě výcviku. Všech 18 pozvaných psovodů bylo rozděleno do tří skupin, které operovaly v místě nasazení a samostatně plnily zadané úkoly. Jejich transport na místa nasazení byl prováděn pomocí vojenské techniky, týlové zabezpečení se podobalo polním podmínkám.

Memorandum o spolupráci mezi HZS ČR a německou THW

V pátek 30. srpna 2013 podepsal generální ředitel Hasičského záchranného sboru ČR plk. Ing. Drahoslav Ryba společně s prezidentem Spolkové organizace technické pomoci (dále jen „THW“) Spolkové republiky Německo Albrechtem Brömmem Memorandum o spolupráci. Podpisu byl přítomen také prezident Spolkové republiky Německo Joachim Gauck. Intenzivní spolupráce mezi HZS ČR a THW byla zahájena v roce 2001. Uskutečněno bylo několik společných cvičení (např. Albis 2008), záchranáři z THW pomáhali v ČR při povodních v srpnu roku 2010, v roce 2011 a 2012 byly uspořádány v SRN kurzy zpevnění a stabilizace budov. Zajímavostí je, že účastník tohoto kurzu úspěšně velel při zásahu a zpevňování budovy výbuchem plynu zříceného domu v Divadelní ulici v Praze v dubnu 2013.
Memorandum vychází ze smlouvy mezi Českou republikou a SRN o vzájemné pomoci při katastrofách a velkých haváriích. Vyjadřuje připravenost HZS ČR i THW nadále prohlubovat vzájemné vztahy a poskytovat si pomoc v případě mimořádných událostí a přípravy na ně.

Září

Seminář o národní kritické infrastruktuře a cvičení Safeguard
Na Krajském vojenském velitelství Ostrava proběhl 10. 9. 2013 seminář o bezpečnostní problematice národní kritické infrastruktury. Seminář seznámil laickou i odbornou veřejnost s činností a rolí české přenosové soustavy v provázaném systému energetických společností.
Při pravidelných cvičeních s tématikou bezpečnosti kritické infrastruktury trénují spolupráci Aktivní zálohy a vojáci štábů KVV společně se složkami Integrovaného záchranného systému. Díky cvičením s názvem Safeguard jsou na zabezpečení, střežení a řešení krizové situace v přímé blízkosti zařízení přenosové soustavy dobře připraveni. Loňské společné cvičení proběhlo 10. 9. u transformovny Albrechtice nedaleko Ostravy.

Cvičení RESTART 2013
Dne 4. září 2013 proběhlo dosud nejrozsáhlejší elektroenergetické cvičení, které se v České republice kdy konalo. Více informací o něm naleznete ve speciálním exkurzu v kapitole „Energetická bezpečnost“ v první části této zprávy.

Česká policistka se účastnila mezinárodního cvičení agentury FRONTEX
Ve dnech od 16. 7. do 12. 8. 2013 se pod názvem REX 2013 uskutečnilo na vnějších pozemních hranicích Maďarska a Rumunska cvičení členů Evropské pohraniční stráže v rámci mechanismu tzv. rychlé intervence, jehož se zúčastnila policistka ICP Praha Ruzyně.
Cvičení se uskutečnilo v rámci mechanismu tzv. rychlé intervence, který je koordinován agenturou Frontex. Jedná se o legitimní proces na základě článku 8d (2) nařízení o Frontexu, kdy jeden nebo více členských států EU může požádat agenturu Frontex o rychlou operativní pomoc v případě nečekaného a masivního nárůstu ilegální migrace na jejich vnějších hranicích. Agentura Frontex má podle stejného nařízení za povinnost pravidelně organizovat taková cvičení tak, aby byla spolu s dalšími členskými státy EU lépe připravena na případy nečekané migrační situace na vnějších hranicích. A tím se de facto prakticky připravovat na nepředvídané vyslání členů týmu Evropské pohraniční stráže do společných operací. Přesto, že se jednalo „pouze“ o cvičení, vyslaní členové týmu vykonávali běžné operativní úkoly a úkony spojené s ochranou pozemní hranice, a to s ohledem na skutečnost, že se v dané oblasti delší dobu zhoršila migrační situace. Aktivace mechanismu nasazování členů týmu Evropské pohraniční stráže v rámci tzv. rychlé intervence efektivně prověřila na jedné straně administrativu a logistiku agentury Frontex a na straně druhé prověřila akceschopnost mechanismu vyslání členů týmu Evropské pohraniční stráže, v jednotlivých zemích Evropské unie.

Mistrovství České republiky záchranných psů a psovodů složek IZS

Ve dnech 13. – 15. 9. 2013 v Plumlově a v Prostějově konalo 9. Mistrovství České republiky záchranných psů a psovodů složek integrovaného záchranného systému. Letošní ročník pořádala z pověření MV – generálního ředitelství Hasičského záchranného sboru České republiky Záchranná brigáda kynologů Jihomoravského kraje. Během mistrovství mezi sebou změřilo síly celkem 12 družstev z České republiky, včetně soutěžního týmu ze Spolkové republiky Německo. Mistrovství bylo slavnostně zahájeno v pátek 13. 9. 2013 v areálu autocampingu Žralok u Plumlovské přehrady, kde také v sobotu 14. 9. 2013 proběhlo slavnostní vyhlášení výsledků a ukončení mistrovství.
Praktické nasazení záchranných týmů probíhalo nepřetržitě, od pátku 21:00 hod do soboty 16:00 hod. Každý tým prováděl jedno denní a jedno noční nasazení. Prostory pro sutinové a plošné vyhledávání byly vždy vedle sebe tak, aby soutěžící mohli provádět činnost současně na obou stanovištích (první kynolog na sutině, druhý kynolog na ploše), a byl pro ně stanoven stejný časový limit.

Mistrovství České republiky v TFA
18. září se na Andrlově Chlumu v Ústí nad Orlicí konalo šesté Mistrovství České republiky v nejtěžších hasičských disciplínách v TFA, z anglického Toughest Firefighter Alive, což v překladu znamená, nejtvrdší hasič přežívá. Soutěž pořádalo MV – generální ředitelství Hasičského záchranného sboru České republiky, Hasičský záchranný sbor Pardubického kraje a Sportovní klub hasičů Ústí nad Orlicí. Celá akce byla pod záštitou hejtmana Pardubického kraje Martina Netolického. V rekordním čase 4.47,23 minut zvládl všechny náročné disciplíny dvojnásobný mistr světa a šestinásobný Mistr Evropy Lukáš Novák. Ke svým světovým titulům si tak dnes konečně připsal i titul mistra České republiky.

Říjen

Vláda schválila novou Koncepci ochrany obyvatelstva

Dne 23. října 2013 schválila vláda ČR svým usnesením č. 805 Koncepci ochrany obyvatelstva do roku 2020 s výhledem do roku 2030. Tato nová koncepce popisuje systém ochrany obyvatelstva v celé šíři a definuje její nejvýznamnější oblasti a nástroje, kterými je realizována.

Základním podkladem pro zpracování Koncepce byly výsledky provedené SWOT analýzy doplněné o další párová porovnání. Tato analýza byla zpracována ve spolupráci za aktivní účasti odborných pracovníků ústředních správních úřadů a územních orgánů. Byla identifikována slabá místa systému ochrany obyvatelstva a navrženy úkoly a opatření pro jejich odstranění. Výsledkem práce bylo nalezení a popsání dvaceti čtyř základních úkolů ochrany obyvatelstva, které budou směřovat k naplnění definovaných strategických priorit: občan, soukromé subjekty, ochrana kritické infrastruktury, věda, výzkum, inovace a vydefinování nových úkolů a přístupů. Realizace těchto úkolů je efektivně rozložena do následujících sedmi let a zároveň je stanovena strategická linie vývoje této oblasti do roku 2030. Cílem je posílení systému ochrany obyvatelstva s maximálním využitím stávajících kapacit a využitím kapacit nových.

Cvičení leteckých záchranářů u teplárny Trmice

Z vrcholu 220 metrů vysokého komína trmické teplárny byly za asistence vrtulníku evakuovány zraněné osoby. Jednalo se o cvičení leteckých záchranářů střediska Letecké záchranné služby v Ústí nad Labem. Výcvik simuloval evakuaci občanů nebo pracovníků postižených náhlým zhoršením zdraví nebo úrazem z výškové budovy či komína.

Ještě před samotným příletem vrtulníku zabezpečili členové Hasičského záchranného sboru Teplárny Trmice ochranný prostor pod komínem. Následně pak v rámci cvičení přiletěl vrtulník se dvěma záchranáři. První slanil na horní ochoz, kde se zajistil proti pádu, druhý slanil za ním. Vrtulník se od komína vzdálil a zůstal v blízkém vizuálním kontaktu ve výšce okolo 230 metrů nad terénem. Na pokyn záchranářů přiletěl vrtulník a s pomocí podvěsového lana evakuoval jak záchranáře, tak figuranta (zraněného) do bezpečí – na plochu na břehu jezera Milada v Chabařovicích. Postup se opakoval po oba dny do vystřídání všech záchranářů. Výcviku se účastnilo na tři desítky záchranářů, hasičů i pracovníků horské služby.

Cvičná nehoda na silnici I. třídy u Znojma

1. října 2013 se na silnici I. třídy mezi obcemi Olbramkostel a Kravsko na Znojemsku konalo cvičení složek integrovaného záchranného systému. Kolem 10. hodiny byla nahlášena havárie osobního automobilu, autobusu a dodávky. Operační středisko Hasičského záchranného sboru vyslalo na místo jednotky ze Znojma a Hrušovan nad Jevišovkou a dobrovolné hasiče z Jevišovic a Suchohrdel. Z Brna vzlétnul vrtulník Policie ČR s posádkou leteckých záchranářů, kteří disponují vybavením pro zásah u dopravních nehod.

Hasiči měli za úkol zajistit místo nehody, třídit a vyprostit lidi z havarovaných vozidel. Velitel zásahu se musel vypořádat s velkým množstvím zraněných. Bylo nutné vytvořit týlový prostor pro práci posádek zdravotnické záchranné služby a umožnit rychlý transport zraněných do nemocnic. Záchranná služba odvezla celkem 37 zraněných. Mrtvé řidiče autobusu a nákladního vozu vystříhávali hasiči po zadokumentování nehody policií. Její vrtulník také hledal dva cestující, kteří od nehody odešli směrem k nejbližší vesnici. Do akce se zapojil i psycholog Hasičského záchranného sboru. Celkem cvičilo na 170 osob napříč různými složkami IZS (včetně např. Správy a údržby silnic a oblastní charity Znojmo).

Mezinárodní cvičení pořádkových jednotek policie ve východních Čechách

Dvoudenní součinnostní cvičení Pořádkové jednotky Krajského ředitelství policie Pardubického kraje s mezinárodní účastí proběhlo v září hned na několika místech východních Čech.
Prvního dne se kromě zmíněné krajské pořádkové jednotky účastnili v rámci dlouhodobé intenzivní spolupráce také policisté z pořádkových jednotek z Německa a Polska. Celkem 50 policistů, z toho 10 z Polska a 10 z Německa, absolvovalo na výcvikovém polygonu Báňské záchranné služby v Odolově na Trutnovsku zaměstnání zaměřené na extrémní situace, se kterými se během svého nasazení mohou setkat. Výcvik orientace ve tmě či záchrana kolegy v extrémních podmínkách lze chápat jako přípravu na situace, kterým mohou být policisté pořádkových jednotek vystaveni například během povodní. Trénink zvyšování především psychické odolnosti pak přispívá ke zdárnému splnění zadaného úkolu během ostrého nasazení.
Předávání zkušeností a znalostí, nácvik a zdokonalení spolupráce a činnosti pořádkových jednotek probíhalo druhý den v Pardubicích. Kromě výše zmíněných složek se druhého dne součinnostního cvičení účastnili také policisté ze Speciální pořádkové jednotky Krajského ředitelství policie hlavního města Prahy a družstvo pořádkové jednotky Městské policie Pardubice. Celkem se tak v místě konání sešlo na 200 policistů včetně služebních kynologů či antikonfliktních týmů.
Stěžejním tématem druhého dne cvičení byla problematika pravicového a levicového extrémismu, diváckého násilí a zákrok pod jednotným velením směřující k udržení veřejného pořádku a ochraně majetku, zdraví a života osob. Policisté si tak navzájem předávali zkušenosti a cvičili rozmanité situace, se kterými se během své činnosti setkávají, jako jsou více či méně poklidné pochody radikálů, napadení demonstrace, vyklizení squatu nebo zákrok na koncertu skupin s extrémistickým zaměřením.

Listopad

Cvičení BLANÍK 2013
Vnitrostátní cvičení s názvem „BLANÍK 2013“ proběhlo na několika místech České republiky, zejména v Praze a Karlových Varech ve dnech 27. – 29. 11. 2013. Více informací o této události naleznete ve speciálním oddíle v úvodu této kapitoly.

Nové operační středisko Královéhradeckého kraje
Dne 15. 11. 2013 ve 13:30 se slavnostně otevřelo Integrované operační středisko na Krajském ředitelství policie Královéhradeckého kraje. Krajské ředitelství Královéhradeckého kraje je jako první v republice, kde je integrované operační středisko vybaveno moderní technologií za účelem zvýšení efektivity operačního řízení Policie ČR v rámci Integrovaného záchranného systému. Důvodem vzniku projektu bylo potřeba včasné a efektivní reakce na zvyšující se hrozby či následky přírodních a technologických rizik, které lze eliminovat či řešit prostřednictvím zajištění vysoké úrovně akceschopnosti a efektivity operačního řízení Policie ČR v rámci IZS. Jedná se zejména o potřebu včasného zásahu na místě mimořádné události.
Projekt je zaměřen na pořízení nové technologie pro operační řízení umožňující zajistit kvalitnější informace pro vytěžení informací z tísňového hovoru, vyšší účinnost operačního řízení a nasazování sil a prostředků, zvýšení přehledu o operační situaci, zkrácení přepravních časů sil a prostředků a dále zajistit interoperabilitu na úrovni jednotlivých krajů a mezi ostatními základními složkami IZS.

Simulovaný požár na vodní elektrárně Orlík

Simulovaný požár v důsledku zkratu a zahoření kabeláže, únik zplodin a vyhledání a transport dvojice zraněných provozních elektrikářů ze suterénu – to byly hlavní body havarijního cvičení, které proběhlo 26. listopadu 2013 v největší české klasické vodní elektrárně na Orlíku.
Hasiči museli zvládnout především lokalizaci a transport dvojice „zraněných“ pracovníků ze zakouřených prostor 2. suterénu.
Havarijní cvičení se zaměřilo na reakci obsluhy a členů havarijního štábu provozu VE Orlík na vznik mimořádné události a činnost při ní. Došlo také na kontrolu funkčnosti technických prostředků pro varování a vyrozumění osob na VE Orlík a činnosti související se zajištěním evakuace osob. Stejně tak byla prověřena správnost a aktuálnost kontaktů v havarijním plánu a spolupráce obsluhy a havarijního štábu provozu VE Orlík. Havarijní cvičení na VE Orlík bylo poslední akcí podobného druhu v roce 2013. Od ledna proběhla cvičení na dvanácti klasických a devíti vodních elektrárnách Skupiny ČEZ.

Prosinec

Policie zdokonaluje operační střediska
Operační středisko Policejního prezidia čeká v roce 2014 velká změna: rekonstrukce a stěhování. Nové prostory se pro operační důstojníky, kteří doposud sídlí v Olšanské ulici, začínají připravovat v budově Policejního prezidia.
Přestavba se uskuteční ve dvou rovinách – technologické, jejímž cílem je modernizace hardwaru i softwaru, a stavební. Z toho důvodu prezidium vyhlásilo 21. ledna 2014 zakázku na dodavatele potřebných stavebních úprav (informace k této zakázce jsou k dispozici na elektronickém tržišti www.softender.cz**)**. Díky projektu, který vede k integraci všech operačních středisek, prošla větší či menší rekonstrukcí už téměř všechna krajská operační střediska.
Hlavním cílem rekonstrukcí je sladění Národního informačního systému celého Integrovaného záchranného systému a dosažení ještě větší efektivity operačního řízení. Nové technologie napomáhají policejní službě jak v každodenních situacích, tak u mimořádných krizových událostí. Budování operačního střediska je totiž součástí projektu *„Jednotná úroveň informačních systémů a operačního řízení a modernizace technologií pro příjem tísňového volání základních složek IZS.“* To jednoduše řečeno znamená, že podobné technologie budou mít i záchranáři, hasiči a další složky integrovaného systému a spolupráce se tím podstatně zrychlí a zdokonalí.
Ukončení projektu, který z 85 % financují evropské fondy, se plánuje na polovinu roku 2014.

Nová výjezdová základna záchranky ve Stodůlkách
Pražská záchranka převzala novou výjezdovou základnu. Kontejnerový objekt je umístěn u páteřní Jeremiášovy ulice, na křižovatce ulic Vackova a Oistrachova ve Stodůlkách. Pro místní obyvatele znamená zlepšení dostupnosti přednemocniční neodkladné péče a zkrácení dojezdových časů posádek k pacientům.

Tří set tisíc lidí se v USA dotkla průmyslová havárie, která kontaminovala pitnou vodu
Zhruba 300 000 Američanů dostalo od úřadů varování, aby nepili vodu z kohoutku, ani ji nepoužívali k mytí a vaření. Guvernér státu Západní Virginie vyhlásil stav nouze poté, co do řeky Elk uniklo z místního závodu asi 5 000 galonů agresivního činidla 4-methylcyklohexan, které se používá k čištění uhelné rudy. V několika okresech došlo k uzavření škol, restaurací a barů. Během několika hodin od oznámení havárie místní lidé vykoupily veškeré zásoby balených vod a plastových kanystrů, na mnoha místech se tvořily dlouhé fronty. S řešením krize pomáhala i Národní garda a federální Úřad pro mimořádné situace. Zkušenosti z této mimořádné situace mohou být využity pro krizové plánování i v České republice.

Zdroje pro tuto kapitolu: MV-GŘ HZS ČR, PČR, telegraph.co.uk, zzshmp.cz

NOVINKY V LEGISLATIVĚ ČR ZA SLEDOVANÉ OBDOBÍ

Energetika a energetická bezpečnost

Předpis 78/2013 Sb., **o energetické náročnosti budov**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=79679&fulltext=&nr=&part=&name=2013&rpp=50#local-content

Předpis 165/2013 Sb., **o druzích ropy a skladbě ropných produktů pro skladování v nouzových zásobách ropy**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=80087&fulltext=&nr=&part=&name=2013&rpp=50#local-content

Předpis 194/2013 Sb., **o kontrole kotlů a rozvodů tepelné energie**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=80187&fulltext=&nr=&part=&name=2013&rpp=50#local-content

Předpis 288/2013 Sb., **o provedení některých ustanovení zákona o integrované prevenci**
http://portal.gov.cz/app/zakony/zakonPar.jsp?page=0&idBiblio=80552&recShow=0&fulltext=&nr=&part=&name=2013&rpp=50#parCnt

Předpis 310/2013 Sb., **změna zákona o podporovaných zdrojích energie**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=80610&fulltext=&nr=&part=&name=2013&rpp=50#local-content

Předpis 350/2013 Sb., **změna vyhlášky, kterou se stanoví technické parametry obnovitelných zdrojů**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=80610&fulltext=&nr=&part=&name=2013&rpp=50#local-content

Předpis 168/2013 Sb., **o nakládání s těžebním odpadem**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=80090&fulltext=&nr=&part=&name=2013&rpp=50#local-content

Předpis 152/2013 Sb., **o celkovém množství elektřiny a plynu spotřebovaném v ČR v roce 2012**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=80054&fulltext=&nr=&part=&name=2013&rpp=50#local-content

Bezpečnost finančních institucí

Předpis 99/2013 Sb., **kterým se mění některé zákony v oblasti pojišťovnictví a penzijního připojištění v souvislosti se změnami v právu EU**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=79841&fulltext=&nr=&part=&name=2013&rpp=50#local-content

Předpis 346/2013 Sb., **o předkládání výkazů bankami a pobočkami zahraničních bank v České republice**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=80770&fulltext=&nr=&part=&name=2013&rpp=50#local-content

Předpis 243/2013 Sb., **o investování investičních fondů a o technikách k jejich obhospodařování**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=80345&fulltext=&nr=&part=&name=2013&rpp=50#local-content

Předpis 253/2013 Sb., **kterým se stanoví podmínky tvorby povinných minimálních rezerv**
http://portal.gov.cz/app/zakony/zakonPar.jsp?page=0&idBiblio=80356&recShow=0&fulltext=&nr=&part=&name=2013&rpp=50#parCnt

Předpisy 468/2013 a 469/2013 Sb., **o změně vyhlášky o účetnictví pro banky a pojišťovny**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=81282&fulltext=&nr=&part=&name=2013&rpp=50#local-content

Informační technologie a kyberbezpečnost

Předpis 214/2013 Sb., **změna zákona o elektronických komunikacích**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=80243&fulltext=&nr=&part=&name=2013&rpp=50#local-content

Krizové řízení

Předpis 307/2013 Sb., **o povinném značení lihu**
http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=80607&fulltext=&nr=&part=&name=2013&rpp=50#local-content

KONFERENCE A SETKÁNÍ

Připravované akce v ČR a v SR v příštím roce

Energetika a energetická bezpečnost

26. – 29. 3. 2014	**RACIOENERGIA** 24. mezinárodní veletrh využití energie Bratislava – Incheba, Slovensko http://www.incheba.sk/#&panel1-1
8. – 9. 4. 2014	**ČEPKON 2014** a **Plynárenství v ČR a SR 2014** Energetický trh pod tlakem regulace a legislativních změn Dorint Hotel Don Giovanni, Praha http://www.konference.cz/akce/detail-2953-CEPKON-2014/
15. – 17. 4. 2014	**Teplárenské dny 2014** Mezinárodní odborná výstava techniky a technologií pro dálkové zásobování teplem a chladem, elektroenergetiku Kongresové centrum Aldis, Hradec Králové http://www.teplarenske-dny.cz/cs/
21. 5. 2014	**EnergoWorld 2014** Informační a komunikační technologie v energetice Praha http://eventworld.cz/akce/energoworld-2014-73/call-for-papers-energo-world-2014
27. – 28. 5. 2014	**Finanční a matematické modely v energetice** Seminář k analýze rizik na energetických trzích Dorint Hotel Don Giovanni, Praha http://www.konference.cz/akce/detail-2805-Financni-a-matematicke-modely-v-energetice/
16. – 20. 9. 2014	**FOR ELEKTRON** 4. mezinárodní veletrh elektrotechniky, automatizace a energetiky PVA EXPO Letňany, Praha http://www.electroncz.cz/

Bezpečnost finančních institucí

25. – 26. 2. 2014	**ICT ve finančních institucích** Konference, mj. zajištění informační bezpečnosti Hotel Dorint Don Giovanni Praha http://www.konference.cz/akce/detail-2942-ICT-ve-financnich-institucich/

25. – 26. 2. 2014 **Platební styk 2014**
Konference, mj. EU a legislativní změny
Dorint Hotel Don Giovanni, Praha
http://www.konference.cz/akce/detail-2930-PLATEBNI-STYK-2014/

24. 4. 2014 ASIS International
Mezinárodní konference bezpečnostního managementu (KBM)
Hotel Dorint Don Giovanni Praha
http://www.kbm2014.cz/

7. 10. 2014 ExpoNet
Svět informatiky ve finančnictví
Moderní trendy, bezpečnost, nová řešení
Praha
http://financnictvi.expo-net.cz/

Informační technologie a kyberbezpečnost

4. 2. 2014 CESNET
Bezpečný provoz sítí a služeb
Ballingův sál Národní technické knihovny, Praha
http://www.cesnet.cz/sdruzeni/akce/bezpecny-provoz-siti-a-sluzeb/

12. 2. 2014 **Storage World 2014**
Aktuální informace o novinkách v archivaci a správě dat
Praha
http://idg.cz/

19. 2. 2014 **Security 2014**
XXII. ročník konference o IT bezpečnosti
Hotel Aquapalace, Praha
http://www.systemonline.cz/it-security/konference-security-2014-predstavi-aktualni-temata-it-bezpecnosti-z.htm

13. 3. 2014 **IDC IT Security Roadshow 2014**
12. ročník prestižní konference.
Národní muzeum, Praha
http://www.security-portal.cz/page/konference-v%C3%BDstavy

18. 3. 2014 **IT Security Workshop**
Možnosti v oblasti ochrany dat
Praha, pozvánka:
http://www.itsw.cz/

15. 4. 2014 **BI & Big Data Conference**
Big Data, Business Inteligence
Praha
http://www.bicon.cz/

15. – 16. 4. 2014 **Monitoring a ochrana dat a osobních údajů**
Konference ohrožení dat
Hotel Dorint Don Giovanni Praha
http://www.konference.cz/akce/detail-2971-MONITORING-A-OCHRANA-DAT-A-OSOBNICH-UDAJU/

16. 4. 2014 **Security Fórum 2014**
Praktické otázky ICT bezpečnosti
Hotel Diplomat, Praha
http://www.konferenceit.cz/html/security-forum-2014.html

13. 5. 2014 **Bezpečnost v Cloudu**
Praha
http://www.bezpecnostvcloudu.cz/

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

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

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

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

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

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

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

Krizové řízení

5. – 6. 2. 2014 Vysoká škola báňská – Technická univerzita Ostrava
XIII. ročník mezinárodní konference OCHRANA OBYVATELSTVA
Ochrana osob při hromadných kulturních, společenských a sportovních akcích
http://www.vsb.cz/info/?reportId=15945

24. 4. 2014 ASIS International
Mezinárodní konference bezpečnostního managementu (KBM)
Hotel Dorint Don Giovanni Praha
http://www.kbm2014.cz/

15. – 16. 5. 2014 MV-GŘ HZS ČR, VŠB-TU Ostrava
Konference „Management bezpečnosti 2014“
Bílé Poličany

6. – 7. 6. 2014 **Hasičské slavnosti**
Litoměřice – výstaviště
www.zahrada.cech.cz

29. 9. – 3. 10. 2014 **INTERPROTEC**
12. mezinárodní veletrh prostředků osobní ochrany, bezpečnosti práce a pracovního prostředí
Brno – výstaviště
http://www.bvv.cz/imt/

Připravované akce v zahraničí

Energetika a energetická bezpečnost

29. – 31. 1. 2013 **ENERTEC** 2014
Mezinárodní odborný veletrh energie
Lipsko, Německo
http://www.enertec-leipzig.de/

27. – 28. 2. 2014 **4th Annual Smart Grids Smart Cities Forum**
Distribution Management Systems, Grid Security
Varšava, Polsko
http://www.allconferences.com/c/4th-annual-smart-grids-smart-cities-forum-2014-february-27

12. – 13. 3. 2014 **RENEXPO Central Europe**
8. mezinárodní energetický veletrh
Budapešť, Maďarsko
http://www.renexpo-budapest.com/

13. – 15. 5. 2014 **EXPOPOWER** a **GREENPOWER**
Veletrh energetiky a obnovitelných zdrojů
Poznaň, Polsko
http://www.expopower.pl/pl/

28. – 29. 5. 2014 **Russia and China Energy Relations**
Importance for European Energy Security
Londýn, Velká Británie
http://www.allconferences.com/c/russia-and-china-energy-relations-london-2014-may-28

Bankovnictví a finanční bezpečnost

12. – 14. 4. 2014 **FORINVEST 2014**
7. mezinárodní veletrh finančních služeb, investic, pojištění a bankovního sektoru
Valencie, Španělsko

http://forinvest.feriavalencia.com/

Informační technologie a kyberbezpečnost

10. – 14. 3. 2014	**CeBIT 2014** Jedna z největších evropských IT konferencí Hannover, Německo http://www.cebit.de/home
29. 4. – 1. 5. 2014	**CyberSec 2014** 3rd International Conference on Cyber Security, Cyber Warfare and Digital Forensics Lebanese University, Lebanon http://wikicfp.com/cfp/servlet/event.showcfp?eventid=33231&copyownerid=41972
19. – 22. 5. 2014	**CEIC 2014** Latest Development in Digital Investigation Hotel Caesars Palace, Las Vegas, USA http://www.htcia.org/2013/07/ceic-2014/
2. - 7. 8. 2014	**Black Hat USA 2014** Konference o kybernetické bezpečnosti a fenoménu hackingu Mandalay Bay, Las Vegas, USA http://www.blackhat.com/us-14
22. – 25. 9. 2014	**36th International Conference of Data Protection and Privacy Commissioners** A New Data Protection e-World Order: Must or Myth? Port Luis, Mauricius http://www.privacyconference2014.org/
14. – 17. 10. 2014	**Black Hat Europe 2014** Konference o kybernetické bezpečnosti a fenoménu hackingu Amsterdam, Nizozemsko http://www.blackhat.com/eu-14/

Krizové řízení

19. – 20. 2. 2013	**FeuerTRUTZ 2014** Odborný veletrh protipožární prevence Norimberk, Německo http://www.feuertrutz-messe.de/en/
2. – 4. 4. 2014	**ISC WEST** Mezinárodní výstava a konference bezpečnostních systémů a vybavení Las Vegas, USA http://www.iscwest.com/
8. – 11. 4. 2014	**SECUREX 2014** Mezinárodní veletrh bezpečnostní techniky Poznaň, Polsko www.securex.mtp.pl
9. – 11. 4. 2014	**SAWO 2014** Mezinárodní veletrh bezpečnosti práce, požární techniky a záchranářství Poznaň, Polsko http://sawo.mtp.pl/pl/

Zdroje použité pro monitoring

MV, PČR, HZS ČR, MPO, MO, MZV, ČTK, vlada.cz, idnes.cz, ceps.cz, cez.cz, mero.cz, pressweb.cz, energetickakoncepce.cz, prumysl.cz, ČT 24, ČRo, net4gas.cz, cepsr.com, banktech.com, lidovky.cz, tpeb.cz, euraktiv.cz, 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, cleverandsmart.cz, technet.idnes.cz, aktualne.centrum.cz, ceskatelevize.cz, enviweb.cz, tretiruka.cz, cyprus-mail.com, prumysl.cz, europol.europa.eu, aphaia.co.uk, allpremium4.blogspot.com, zive.cz, e15.cz, trustport.com, telegraph.co.uk, zzshmp.cz, kickstarter.com, interpol.int, hpsolutions.cz, bakerstreet.wikia.com, cnb.cz, newmoney.gov, ppas.cz, economist.com, csoonline.com, edition.cnn.com, enisa.europa.eu, en.wikipedia.org, tomshardware.com, stanford.edu, chip.cz, newscientist.com, russelwebster.com, businessworld.cz, infoworld.com, europa.eu, itnewsafrica.com, scmagazine.com.au, businessinsider.com, rozhlas.cz, reko a.s., atominfo.cz, bihdaytonproject.com, eon.cz, elektrika.cz, spiegel.de.

Zdroje obrázky

obrázky byly čerpány z výše uvedených zdrojů + ze zdrojů:

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

Text neprošel jazykovou a stylistickou úpravou.