Ohrožení průmyslového závodu během 25 sekund

Výtahy, topení nebo systémy pro hašení požáru – hackeři je v průmyslových závodech dokážou ovládnout během několika málo sekund.

Když bezpečnostní výzkumníci Billy Rios a Terry McCorkle skončili na Kaspersky Security Analyst Summitu svou řeč, nikdo nepochyboval, že by během 25 sekund dokázali získat kontrolu nad celou řadou důležitých zařízení v průmyslových závodech. Pomocí skriptu, který předvedli, by klidně mohli (jako teroristé) v továrně na druhém konci světa zajistit přehřátí topných systémů a tím způsobit požár – samozřejmě až poté, co nejprve deaktivovali hasicí systémy. Rios a McCorkle jsou specialisté na systémy s Niagara Frameworkem – to je systémová platforma, která integruje různé systémy a zařízení bez ohledu na výrobce nebo komunikační protokol do jednotné platformy, která může být snadno řízena a kontrolována v reálném čase přes internet pomocí standardního webového prohlížeče. Pomocí vyhledávače lze snadno zjistit, jak moc je využití této platformy rozšířené – v současnosti lze přes internet ovládat přes 21 500 komplexů.

Výše uvedený trik však není žádnou novinkou: například v loňském roce našli hackeři podobnou slabinu v systému sesterského koncernu Siemens – v softwaru od firmy RuggedCom, která buduje řídicí systémy pro dopravní systémy. V něm totiž existoval nedokumentovaný účet administrátora, který nemohl být odstraněn a který byl chráněn jedním zadaným heslem.

SVÉ SYSTÉMY AKTUALIZUJE MINIMÁLNÍ POČET FIREM

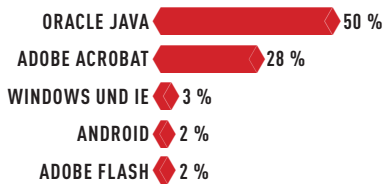
Podle Billyho Riose nespadá většina kontrolních systémů pod vliv IT oddělení. To vysvětluje, proč mnoho společností stále ještě nevyužívá dostupné záplaty pro řídicí systémy. Fakt je, že existujících mezer je opravdu hodně. Například v roce 2012 bylo výrobcům různých systémů nahlášeno více než 1 000 kritických slabých míst. Není také pochyb, že ne každý hacker nalezenou zranitelnost firmě ohlásí.

Rychlý a efektivní

Hackeři předvedli svůj skript pro útok na Kaspersky Security Analyst Summitu.

HACKEŘI MILUJÍ TYTO PROGRAMY

V roce 2012 bylo 50 procent všech malwarových útoků na počítače uživatelů provedeno přes mezery v Javě.



ZDROJ: KASPERSKY

Antiviry: 400% nárůst

Obchod Alza.cz zaznamenal nebývalý zájem o licence antivirových programů, který může souviset s DDoS útoky. Manažer nákupu Alza.cz Petr Hrabal k tomu dodává: *„Těší nás zodpovědnost a chování našich zákazníků, kteří nechtějí podcenit vzniklou situaci. Je vidět, že povědomí o nebezpečí virové nákazy počítače je už nyní velmi vysoké."*

90 % útoků začíná spear phishingem

Podle nových dat za období únor až září, které shromáždila bezpečnostní společnost Trend Micro, stojí na počátku celých 91 % cílených útoků e-mail se spear phishingem. To je typ phishingu, při kterém podvodné e-maily zasílané s cílem získat citlivá data využívají informace o cílovém objektu, aby byl útok konkrétnější a osobnější. Namísto obecných oslovení, jako je tomu u běžných phishingových kampaní, se tak v e-mailech objeví například jméno příjemce, jeho pracovní zařazení nebo funkce. Konečným cílem útoku je přinutit oběť, aby buď otevřela škodlivý soubor v příloze e-mailu, nebo aby klikla na odkaz směřující na podvodný web s malwarem či specializovanými exploity.

DATOVÉ ÚNIKY MĚSÍCE

AMERICKÁ EMISNÍ BANKA: ZMIZELO 4 000 OSOBNÍCH DAT

V noci ze 4. února 2013 získali útočníci přístup k interní síti americké emisní banky Fed. Ukradeno a zveřejněno na internetu bylo více než 4 000 údajů o bankovních zaměstnancích – včetně poštovní a e-mailové adresy, mobilního a faxového číslo. Zdá se, že kooordinátorem akce byla skupina Anonymous, která tak chtěla protestovat proti vyšetřování hackera Aarona Schwartze.

VISA: ODCIZENO 11 MILIONŮ DOLARŮ

Počítačoví zločinci ukradli prostřednictvím manipulací s limity karet kolem 11 milionů dolarů. Hackeři dokázali zvýšit denní limit u předplacených karet, což normálně není možné. Díky tomu mohli na jednu kartu čerpat až 500 000 dolarů. Útočníci získali pomocí SQL injection a hacku hesla přístup do vnitřní sítě, která povoluje VISA platby. Další podrobnosti o útoku a škodách VISA nezveřejnila.

TWITTER: HACKNUTO 250 000 ÚČTŮ

Podle provozovatele mikroblogovácí služby Twitter získali neznámí hackeři údaje přibližně 250 000 uživatelů. Odcizena byla uživatelská jména, e-mailové adresy a hashe hesel. Podle šéfa bezpečnosti Twitteru Boba Lorda nešlo o útok amatérů, ale o profesionální hack – celá záležitost se stále vyšetřuje.

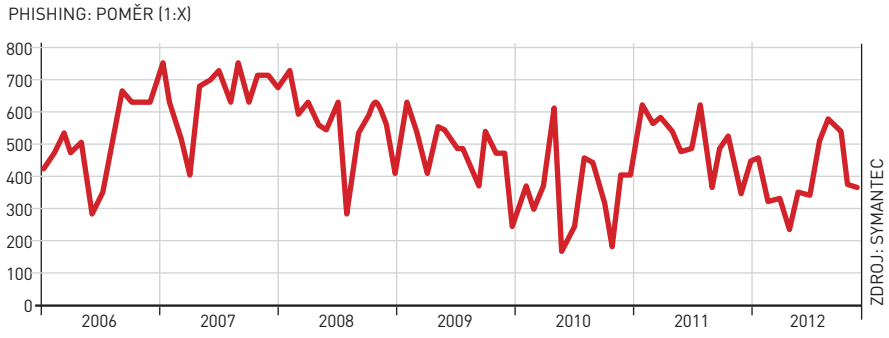
FOTO: THINKSTOCK/HEMERA

7000

ÚTOKŮ DENNĚ NA HRÁČE ON-LINE HER NAPOČÍTALA BEZPEČNOSTNÍ FIRMA KASPERSKY V ROCE 2012.

VÍCE PHISHINGOVÝCH ÚTOKŮ

Klesající křivka naznačuje, že phishingových útoků pomalu, ale jistě přibývá.



Nebezpečný UEFI

Malá manipulace s UEFI BIOS z notebooku Samsung dokáže zničit notebook. Jak předvedl bezpečnostní výzkumník Matthew Garrett, stačí jen změnit speciální proměnnou UEFI v chráněném datovém prostoru. Poté už nelze notebook spustit. Nepomůže dokonce ani vymazání CMOS-bufferu, který obsahuje nastavení BIOS.

Neexistuje žádné bezpečné heslo

Podle studie firmy Deloitte už ani heslo o délce osmi znaků, tvořené z písmen abecedy, čísel a speciálních znaků, které bylo až donedávna považováno za bezpečné, bohužel nestačí. Od té doby totiž výrazně vzrostl výkon počítačů – ty nyní mohou prolomit tato hesla za zhruba šest sekund.

Pokud heslo navíc obsahuje velké začáteční písmeno a na konci čísla, může být jeho prolomení ještě rychlejší. Vědci doporučují používat dvoucestné ověřování, jako například přes heslo a kód v mobilním telefonu.

D-Link bojuje proti zranitelnostem aktualizací

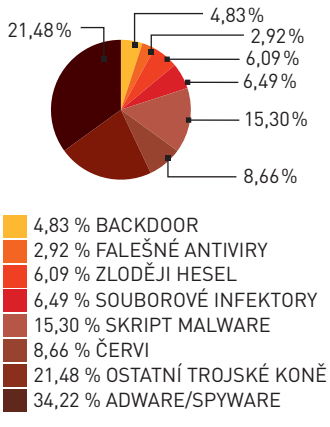
Výzkumník Michael Messner objevil kritickou mezeru v routerech D-Link, která útočníkům umožňuje manipulovat se směrovačem prostřednictvím vzdáleného přístupu. Před používáním směrovačů D-Link DIR-300 a DIR-600 varuje dokonce německý bezpečnostní úřad (LKA). Zpočátku D-Link žádné pochybení nepřipouštěl. Poté, co Messner zveřejnil svou zprávu, začala společnost pracovat na záplatách. Podle firmy mohly za pozdní aktualizace pro routery interní komunikační problémy.

Hrozby na úložištích

Riziko infikování počítače škodlivým softwarem číhá i na domácích webech. Stačí být neopatrný při vyhledávání potenciálně problémových aplikací, a místo programu pro získání výhod v oblíbené on-line hře můžete stáhnout malware, který bude tajně odesílat informace z vašeho počítače útočníkovi. V AVG Virus Lab vyzkoušeli například vyhledávání programu pro podvodné získání herní měny v on-line hře Runescape. Všechny nalezené soubory obsahovaly škodlivý kód a jejich spuštěním by došlo k infikování počítače. Nejčastěji jsou takto maskovány trojské koně, které mají za úkol vylákat přihlašovací údaje oběti ke konkrétní on-line hře a odeslat je útočníkovi.

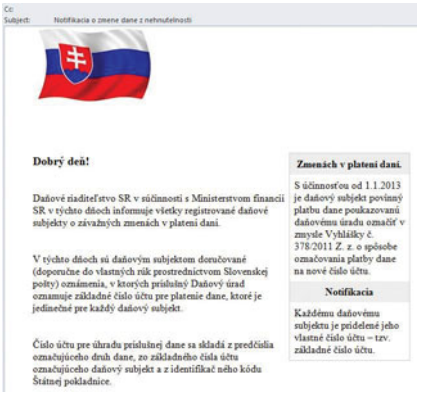
Past v podobě škodlivého softwaru může na uživatele číhat i při vyhledávání filmů. AVG Virus Lab otestovali, jak může vypadat vyhledávání seriálu na populárním stahovacím serveru. Zde byla pro uživatele situace přívětivější a při bližším pohledu na velikost jednotlivých souborů bylo hned zřejmé, které výsledky nebudou obsahovat žádný film. Ve skutečnosti obsahovaly škodlivý kód, tentokrát v podobě tzv. ZeroAccess rootkitu. Při neznalosti problematiky (v kombinaci s neaktuálním antivirovým programem) si tak může uživatel infikovat svůj počítač. Podle Jiřího Kropáče, vedoucího AVG VirusLab, lze podobný trend očekávat i v letošním roce – mezi největší hrozby bude například patřit trojský kůň FakeAlert nebo malware Sirefef.

MALWARE V ČR V ROCE 2013



Slováky ohrožuje „daňový“ trojský kůň

Antivirová společnost Eset varovala slovenské firmy i veřejnost před podvodným e-mailem, pod kterým je podepsán daňový úřad.


Cc:
Subject: Notifikacia o zmene dane z nehnuteľností

Dobrý deň!

Daňové riaditeľstvo SR v súčinnosti s Ministerstvom financií SR v týchto dňoch informuje všetky registrované daňové subjekty o závažných zmenách v platení dani.

V týchto dňoch sú daňovým subjektom doručované (doporučne do vlastných rúk prostredníctvom Slovenskej pošty) oznámenia, v ktorých príslušný Daňový úrad oznamuje základné číslo účtu pre platenie dane, ktoré je jedinečné pre každý daňový subjekt.

Číslo účtu pre úhradu príslušnej dane sa skladá z predčísla označujúceho druh dane, zo základného čísla účtu označujúceho daňový subjekt a z identifikač ného kódu Štátnej pokladnice.

Zmenách v platení dani.

S účinnosťou od 1.1.2013 je daňový subjekt povinný platbu dane poukazovanú daňovému úradu označiť v zmysle Vyhlášky č. 378/2011 Z. z. o spôsobe označovania platby dane na nové číslo účtu.

Notifikacia

Každému daňovému subjektu je pridelené jeho vlastné číslo účtu – tzv. základné číslo účtu.

Ve skutečnosti jde o zprávu od neznámého odesílatele, který se oběť pokouší navést k tomu, aby si stáhla jistý dokument. Jestliže jednotlivci nebo firmy trik neprohlédnou, nainstalují si tímto způsobem do systému trojského koně, který z jejich počítačů může získávat citlivé informace v podobě přístupových údajů do různých webových služeb, včetně internetového bankovnictví.

Tzv. phishingový e-mail upozorňuje na fakt, že daňové subjekty musí daň uhradit na číslo účtu, které je jedinečné pro každého plátce daní. Odesílatel zprávy tvrdí, že podrobný popis tohoto jedinečného čísla účtu se nachází v dokumentu, který si může adresát stáhnout z konkrétní webové adresy. Na té se však skrývá trojský kůň.

„Útočník zneužívá období, ve kterém daňové subjekty platí daně, a také fakt, že již druhý rok úhradu provádějí převodem na číslo účtu, které je pro každý subjekt jedinečné. Je tedy pravděpodobné, že některé firmy této zprávě uvěří a škodlivý kód si stáhnou do svého systému,“ říká Petr Šnajdr, specialista na kybernetickou bezpečnost společnosti Eset.

Údaje ze systému Eset Live Grid, který analyzuje data o malwaru, ostatně potvrzují, že trojský kůň se pokusil dostat i do počítačových systémů několika slovenských firem a organizací. To znamená, že zaměstnanci pracující v těchto firmách se nechali nachytat a na nebezpečný odkaz klikli. Do jejich počítačů se však hrozba nenainstalovala, protože Eset Live Grid získává statistické údaje jen od uživatelů svých řešení a ti jsou před tímto trojským koněm chráněni.

„Tento případ potvrzuje, že zajištění firemních systémů není jen záležitostí kvalitního antivirového řešení, ale i odpovědného chování zaměstnanců,“ dodává Petr Šnajdr.

Phishingový e-mail je podepsán daňovým úřadem, e-mailová adresa odesílatele však neodpovídá daňové sekci Finančního ředitelství Slovenské republiky (@drsr.sk) a má úplně jinou koncovku. Zprávu však neodeslal ani skutečný uživatel dané e-mailové adresy, útočník totiž zprávu podvrhl použitím techniky zvané spoofing. Jedná se o odeslání zfalšovaného e-mailu jménem osoby, která si toho není vědoma. E-mail byl kromě toho napsán ve spisovné slovenštině, což mohlo u adresáta potvrdit věrohodnost toho, že jde o důležité úřední oznámení.

Výše popsaný trojský kůň získává citlivé údaje z internetových prohlížečů Internet Explorer, Google Chrome a Mozilla Firefox. Antivirová řešení společnosti Eset hrozbu detekují pod názvem Win32/Sazoora.A, jedná se o stále aktivní infekci.

Antivirové řešení pro Android

Poslední dobou sleduje tým AVG VirusLab nový fenomén. Kyberzločinci již nevykrádají jen skutečné peníze z bankovních kont nebo přihlašovací údaje například z e-mailových schránek, ale zaměřují se také na herní účty. Hráči všech on-line her se proto musejí mít na pozoru.

K odcizení účtu volí kyberzločinci nejrůznější strategie, které jim umožní přelstít nic netušícího hráče. Pro vytipování ideálního terče útoku se zneužívají herní fóra, kde se útočník vydává za neznalého začátečníka a žádá radu. Podle jednotlivých reakcí vytipuje zkušeného hráče na pokročilé úrovni, takže si může si být jistý, že natrefil na uživatele, který má na svém herním kontě o co přijít. Jednoduchými triky se útočníkovi poté podaří dostat do uživatelova počítače malware, který mu vykrade herní účet.

Časté jsou i případy, kdy kyberzločinci provokují ostatní hráče k podvodům – nabízejí jim artefakty, bonusy, vylepšení herní postavy anebo možnost, jak si přivydělat herní měnu. Hráči, který má o tyto neférové praktiky zájem, pak stačí jen on-line zaplatit, předat svoje přístupové údaje do hry anebo z poslaného linku stáhnout a spustit nástroj, který, jak tvrdí útočník, „není běžně dostupný“. Žádné bonusy tak ale nezíská, naopak pošle zcela dobrovolně kyberzločinci hotovost, svoje přístupové údaje do hry, anebo si jen infikoval počítač. Situace je o to horší, že v tomto případě se okradený uživatel ani nenahlásí administrátorovi – sám by se tím usvědčil z podvodu.

Protože podobných útoků neustále přibývá, připravil Jiří Kropáč, člen AVG VirusLab, několik rad, jak se kyberzločincům ubránit a uchránit si v on-line hře herní měnu, virtuální postavu a její získané artefakty:

► Nastavit si bezpečné heslo, odlišné od hesla používaného na hráčských fórech. Hráči by heslo do hry měli pravidelně měnit a nikde jinde jej nepoužívat.

► Pravidelně aktualizovat antivirový i operační systém na nejnovější verzi.

► Dbát maximální opatrnosti při stahování neoficiálních doplňků, jejichž součástí je instalační balíček anebo spustitelné soubory obecně. Vyplatí se počkat, až komunita nově příchozí doplněk otestuje.

► Pečlivě si hlídat transakce na herním účtu a cokoli podezřelého ihned nahlásit administrátorovi hry. Pokud hráč na krádež přijde včas, může ještě mnohé zachránit.

► Je nebezpečné být bezmezně důvěřivý k ostatním zvídavým hráčům a sdělovat jim informace, které by mohli využít ke kyberútoku na váš vlastní herní účet.

Vzhledem k tomu, že některé počítačové hry umožňují on-line nákupy pomocí platební karty, kdy uživatel průběžně například dokupuje herní předměty za skutečnou měnu, je uvážlivost a opatrnost namístě jako u každé on-line platby.

Například 15 000 zlaťáků ve hře World of Tanks stojí přibližně 1 200 Kč. I proto se hackerům útok vyplatí.

Cloud je víc než technologie

Ve využívání IT služeb v cloudu se do popředí dostává problematika bezpečnosti.

Představa, že citlivá firemní data se ukládají na cizích serverech, je pro řadu majitelů firem a jejich IT oddělení naprosto nepřijatelná.

BEZPEČNOST DAT

Bezpečnost je zapotřebí vnímat z několika hledisek. Prvním z nich je schopnost provozovatele cloudu data vhodným způsobem zálohovat. Už v tomto bodě se od sebe přístupy jednotlivých poskytovatelů natolik liší, že rozhodně stojí za to vyžádat si detailní informace.

Další otázkou je, ve kterém státě jsou data fyzicky uložena. V agendách případů, v nichž se například zpracovávají osobní údaje, je zapotřebí, aby data byla umístěna na území Evropské unie, někdy dokonce na území České republiky. Solidní dodavatel dokáže umístění dat garantovat.

Třetí částí zabezpečení dat je jejich přenos. Provider může mít velmi dobře zajištěné datové centrum, ale pokud není dostatečně zabezpečen přenos dat, riziko jejich zneužití roste. Pokud však zákazníkům nabízí datové služby až na úrovni samostatného fyzického datového připojení, je bezpečnost dat v cloudu plně srovnatelná se situací, kdy data neopustí firemní servery.

Navíc v případě, že zákazník nakupuje komunikační služby od jednoho dodavatele, může si na jednom místě pořídit celorepublikovou VPN, datové centrum, zajištění bezpečnosti perimetru nebo řešení hlasové i datové komunikace a často i konkrétní aplikace. Konkrétně u T-Mobile jde v současnosti o Microsoft Office 365, v blízké budoucnosti to budou například účetní programy.

ÚSPORY Z PRUŽNOSTI

Podle slov Miloše Mastníka, ředitele marketingu pro firemní segment ve společnosti T-Mobile, v tomto případě určitě platí, že celková dodávka ICT služeb představuje vyšší hodnotu než součet jednotlivých částí. IT nemusí řešit řadu provozních otázek ani řadu dílčích smluv s jednotlivými dodavateli. Může se tak soustředit na strategické záležitosti, respektive na to, jak mohou technologie pomoci firemnímu byznysu.

SLEVOVÉ SERVERY POHLEDEM PRÁVNÍKA

V minulém vydání Chipu jsme zmínili problémy, s nimiž se mohou spotřebitelé a obchodníci ve spojení se slevovými portály setkat. Nyní se na některé z nich podíváme podrobněji.

JUDr. MARTIN HOUT

Z cela zásadní věcí je v této oblasti informační povinnost, jíž jsou slevové portály a ostatní obchodníci zatíženi a jejímž řádným splněním odpadají i mnohé následné problémy. Rozhodne-li se tak spotřebitel učinit nějaký nákup na slevovém portálu, neměl by mít v zásadě žádné pochybnosti o tom, s kým a kdy přesně smlouvu uzavřel, čeho konkrétně se smlouva týká a jaká jsou práva a povinnosti jednotlivých stran.

Slevy pouze „v pronájmu“

Obchodní podmínky slevových serverů mohou být samozřejmě různé a nelze tak v tomto omezeném prostoru vystihnout vše, nicméně pokud si vezmeme jako příklad model, v němž slevový portál pouze *„pronajímá“* jisté místo na svých stránkách a tvrdí, že není účastníkem smluvních vztahů a že za nic neodpovídá, potom se lze přesto často oprávněně ptát, kdo vlastně smlouvu se spotřebitelem uzavřel, v jakém okamžiku a s jakým obsahem (viz například voucher na večeři, který už spotřebitel zaplatil slevovému portálu, přičemž teprve následně bude upřesněn čas apod.).

Pro názornou ukázku uvěřme výše uvedenému a představme si situaci, kdy slevový portál skutečně *„nebude účasten“* například kupní smlouvy a jeho odpovědnost bude minimální, neboť prodávajícím ve smyslu zákona č. 634/1992 Sb., o ochraně spotřebitele (dále jen „ZOS“), budou jednotliví obchodníci nabízející své zboží a služby. V tomto případě, podívám-li se na různé slevové portály, vidím hned několikeré porušení zákona. Přistoupíme-li totiž na výše uvedené, potom každý jednotlivý podnikatel musí na slevovém portálu informovat spotřebitele například ve smyslu § 53 odst. 4 a odst. 7 občanského zákoníku (dále jen „OZ“) či třeba ve smyslu § 13 ZOS, podle něhož by spotřebiteli měla být vysvětlena i práva spojená s reklamacemi. Skrze ust. § 5 odst. 1 písm. c) a odst. 4 ZOS se potom nesplnění této povinnosti snadno stává nekalou obchodní praktikou či jiným správním deliktem dle téhož zákona, za což by měla být příslušným orgánem uložena pokuta.

Zajímavé je také ust. § 16 odst. 1 ZOS, podle něhož je prodávající povinen vydat doklad o zakoupení služby či zboží, když setkat se lze i s tím, že tento doklad spotřebiteli vydá se svým razítkem právě slevový portál, a to navzdory skutečnosti, že prodávajícím není. Nastává tedy situace, kdy doklad nevydá osoba, která tuto povinnost má, přičemž spotřebitel je navíc *„maten“* tím, že prodávající jsou najednou dva, z nichž jeden jím vlastně vůbec není. I tyto skutečnosti dle mého názoru svědčí o porušování zákona a těžko lze brát jako omluvu to, že vztah portálu a obchodníka by byl ještě složitější (vyúčtování provizí, daňová a účetní problematika apod.).

Není zákazník jako zákazník

V předchozím vydání Chipu také padla zmínka o manipulaci s cenami a rozdílném zacházení se spotřebiteli. Pokud by v rámci slevových akcí došlo k rozlišování mezi zákazníky obyčejnými a těmi ze slevových portálů, mohlo by snadno dojít k diskriminaci spotřebitele dle § 6 ZOS či ke spáchání nekalé obchodní praktiky, neboť měla-li by být sleva kompenzována snížením kvality poskytované služby, ve skutečnosti by se o žádnou slevu nejednalo. Protiprávním jednáním však musí být nutně i různá manipulace s cenami výrobků a služeb, kde můžeme přemýšlet o trestném činu, nekalé obchodní praktice či třeba o porušení § 12 odst. 2 písm. d) ZOS, v němž se praví, že *„informace o ceně nebo okolnost, že informace je neúplná anebo chybí, nesmí zejména vzbuzovat zdání, že cena byla nebo bude zvýšena, snížena nebo nezměněna, i když tomu tak není“*.

Jak tedy vidno, ačkoliv jsme se zabývali pouze právními vztahy mezi obchodníky a spotřebiteli, právních komplikací zde může být skutečně mnoho, přičemž zdaleka ne vždy může být pokuta pro příslušného obchodníka tou poslední nepříjemností, jež ho potká. Zde se tak můžeme krátce vrátit k ust. § 53 odst. 4 a odst. 7 OZ, na jejichž základě může při porušení zákona obchodníkem snadno dojít k tomu, že spotřebitel bude moci odstoupit od mnohých smluv uzavřených *„na dálku“* třeba i v tříměsíční lhůtě (zde však pozor na výjimky z možnosti odstoupit od smlouvy u mnohých produktů, viz ust. § 53 odst. 8 a § 54 OZ).

Jestliže se tedy obchodníci chtějí vyhnout komplikacím, kromě mnohých jiných spotřebitelských ustanovení by měli věnovat pozornost i tomuto konkrétnímu a řádně informovat nejen o sobě a nabízených produktech, ale i o souvisejících detailech. Poněkud univerzálnějšího charakteru je potom například ust. § 49a OZ, podle něhož *„právní úkon je neplatný, jestliže jej jednající osoba učinila v omylu, vycházejíc ze skutečnosti, jež je pro jeho uskutečnění rozhodující, a osoba, které byl právní úkon určen, tento omyl vyvolala nebo o něm musela vědět....“*, což by se mohlo týkat zmiňovaných nekalých praktik a manipulací s cenami.

Bankrot neznamená konec?

A co *„bankroty“* slevových portálů? Představíme-li si, že spotřebitel již obchodníkovi zaplatil za zboží či službu (peníze jakožto své plnění ze smlouvy však uhradil přes *„zástupce“* obchodníka – slevový portál), má potom vůbec bankrot slevového portálu, který již peníze neposlal tam, kam měl, vliv na povinnost obchodníka poskytnout zboží či službu? Odpověď samozřejmě závisí na povaze konkrétních smluvních vztahů, a priori bych se však jako spotřebitel nevzdával. Ačkoliv potom není tento text zdaleka vyčerpávající a rozhodně nepřinesl odpovědi na veškeré možné otázky, přesto věřím, že alespoň trochu otevře oči všem zúčastněným stranám a pomůže jim orientovat se v právech a povinnostech, které současné právní předpisy obsahují.

AUTOR@CHIP.CZ