ZODPOVEDÁ ZA PHISHINGOM UKRADNUTÉ PENIAZE BANKA ALEBO KLIENT?

MARTIN HUSOVEC

Súd:	Krajský súd Trenčín
Dátum:	19.06.2013
Sp. zn.:	17Co/213/2012
Dostupnosť:	blog.eisionline.org[1]; rozhodnutia.sk

V júli 2013 rozhodol Krajský súd v Trenčíne zrejme jeden z prvých prípadov k otázke zodpovednosti banky v prípade, ak sa jej klient stane obeťou phishingu (podvodnej stránky zbierajúcej údaje) kombinovaného so sociálnym inžinierstvom (následným získaním zvyšných údajov od obete).

1. SKUTKOVÝ STAV

V spore klient VÚB prišiel o 3.000 Eur, pretože sa jeho počítač nakazil z neznámych dôvodov vírusom, ktorý do už napadnutého internetového prehliadača klienta pridal škodlivý kód, ktorý pozmenil výsledné chovanie stránky po jej celkovom zobrazení. Podľa informácií VÚB išlo o tzv. Man-in-the-browser útok[2], ktorý využíva zraniteľnosti internetových prehliadačov tým, že vložením škodlivého kódu dokáže úplne zmeniť vonkajšie správanie webstránky tak, že užívateľ nepozorovane spúšťa aj skryté transakcie, ktoré mu nie sú viditeľné. Túto techniku je možné úspešne použiť aj v prípade, ak stránka používa certifikáty ako SSL alebo PKI.

Klient VÚB v tomto prípade teda nevedomky aktivoval v internetovom prehliadači stránku, ktorá sa tvárila ako internetové bankovníctvo VÚB

[1] Rozšírená verzia tejto anotácie bola uverejnená na http://blog.eisionline.org/2013/09/20/zodpoveda-za-pshishingom-ukradnute-peniaze-banka-alebo-klient/

[2] Pozri viac http://en.wikipedia.org/wiki/Man-in-the-browser

banky, no skryto zachytávala poskytnuté údaje. Účelom tejto podvodnej stránky bolo ľsťou vylákať citlivé autentifikačné údaje a následne ich poslať neznámemu páchateľovi. Ten následne telefonicky kontaktoval žalobcu, predstavil sa ako pracovník banky a informoval ho, že banka zaregistrovala pokus o zrealizovanie podozrivej transakcie a na jej zrušenie je potrebné uviesť autentifikačný údaj z SMS správy. Klient banky poskytol tento autorizačný prvok, čím však práve autorizoval platby podvodníka.

Klient síce v zápätí notifikoval banku, no platba už bola realizovaná. Keďže zrejme banka "reklamáciu" neuznala, rozhodol sa banku o ušlé prostriedky zažalovať. Súd musel aplikovať § 12 zákona č. 492/2009 o platobných službách, ktorý upravuje za akých situácií a do akej miery bude stratu niesť sám klient, banka alebo obidva subjekty spoločne. Predmetné ustanovenia sú transpozíciou článku 61 smernice č. 2007/64/ES o platobných službách na vnútornom trhu. Ak by súd ustálil, že klient konal *tzv. ľahko nedbanlivo* pri zabezpečovaní bezpečnostných prvkov, musel by niesť aspoň spoluúčasť až do výšky 100 eur (§ 12 ods. 1 ZPS). Ak by sa preukázalo, že konal *tzv. hrubo nedbanlivo* pri zabezpečovaní bezpečnostných prvkov (§ 12 ods. 2 ZPS), musel by niesť celú stratu úplne sám. Banka pochopiteľne argumentovala, že klient vydaním údajov konal v hrubej nedbanlivosti, pretože porušil svoje zákonné povinnosti (§ 26 ZPS) a primeranú starostlivosť, a preto musí niesť celú stratu sám. Klient zas tvrdil, že konal len ľahko nedbanlivo, a preto má niesť len časť straty (spolúčasť vo výške 100 eur).

Z toho čo uvádza súd je zrejmé, že súd nie úplne správne zistil skutkový stav. Súd v rozhodnutí uvádza:

> [..] žalovaný [VÚB Banka] oznámil písomne žalobcovi [klient VÚB] dňa 01.02.2011, že dňa 05.12.2010 bola z jeho bežného účtu odúčtovaná suma 3.000 Eur. Pri šetrení zistil, že počítač, z ktorého sa do Internet bankingu žalobca prihlasoval, bol infikovaný počítačovým vírusom, ktorý sa do počítača mohol dostať viacerými spôsobmi, nie však cez webstránku VÚB. **Pri infikovaní počítača sa vírus v počítači aktivoval a následne v internetovom prehliadači generoval stránku snažiacu sa napodobniť dizajn stránok internetového bankovníctva VÚB. Účelom tejto podvodnej stránky bolo ľsťou vylákať citlivé**

autentifikačné údaje a následne ich poslať neznámemu páchateľovi. Neprimeraným zabezpečením počítača voči škodlivým vírusom boli dobrovoľne zverené bezpečnostné prvky neznámemu podvodníkovi. Tento sa im neskôr prihlásil pomocou prihlasovacích údajov do Internet bankingu a zadal jednorazovú platbu. Následne kontaktoval žalobcu, predstavil sa ako pracovník banky a informoval ho, že banka zaregistrovala pokus o zrealizovanie podozrivej transakcie a na jej zrušenie je potrebné uviesť údaj - pozíciu GRID karty. Žalobcom poskytnutý autorizačný prvok - pozíciu GRID karty použil páchateľ na autorizáciu zadanej platby. Žalobca potvrdil, že v nedeľu mu osoba, tvrdiac, že je zamestnancom banky, oznámila, že na jeho účte prebiehajú prostredníctvom bankomatovej karty podozrivé operácie a v ten deň mu opätovne telefonovala takáto osoba, opätovne tvrdila, že na jeho účte prebiehajú podozrivé pohyby a za účelom zablokovania kreditnej karty si vyžiadala autentifikačný kód z SMS správy. Tento údaj poskytol a následne na druhý deň, 06.12.2010 uplatnil v banke reklamáciu. Okrem iného vyslovil názor, že tvrdenie o tom, že žalobca nezabezpečil svoj počítač dostatočným autorizovaným programom, žalovaný nepreukázal, pričom nemožno považovať za nedbanlivosť žalobcu tú skutočnosť, ak osobe, ktorá mu v deň pracovného pokoja, oznámi, že na jeho účte prebiehajú podozrivé operácie a zverí mu údaje dôverného charakteru. Bežný klient banky s priemernými znalosťami práce s počítačom nemusí mať dostatok odborných vedomostí k tomu, aby rozpoznal, že pracuje s vírusom vygenerovanou fiktívnou stránkou internetového bankovníctva, alebo aby poznal do podrobností pracovné postupy banky. Žalobca neudelil súhlas s vykonávaním sporných bankových operácii, a preto ich nemožno považovať za autorizované platobné operácie, pričom najbližší možný deň 06.12.2010 uplatnil osobne v banke reklamáciu k pohybom na účte, ku ktorým neudelil súhlas. Práve žalovaný potvrdil, že neoprávnené

> transakcie platobnou kartou boli realizované v čase od 06.12.2010 do 15.12.2010, teda po uplatnenej reklamácii.

Zistený skutkový stav je nesprávny už v tom, že vychadza zo zverenia bezpečnostných prvkov už momentom nedostatočného zabezpečenia počítača. V tejto fáze útoku však bola "len" bez vedomia používateľa neoprávnene pozmenená klientová transakcia (napríklad zmenené číslo účtu príjemcu), pričom nedošlo k odovzdaniu bezpečnostných prvkov. K tomu došlo až následne, pomocou sociálneho inžinierstva zneužitím klientovej dôvery po telefóne. Pochopenie, ktorá skutočnosť bola rozhodujúca pre umožnenie útoku, pritom môže byť rozhodujúce. Keďže však k prípadu s najväčšou pravdepodobnosťou nebol priznaný znalec, ostávajú niektoré skutkové otázky z rozhodnutia otvorené.

Podľa dostupných informácií sa teda zdá, že klient banky sa útoku mohol vyhnúť jednak tým, že by ochránil svoj počítač od vírusu, napríklad používaním antivírusu, resp. aj tým, že by využíval bezpečný a udržiavaný internetový prehliadač bez zneužiteľných zraniteľností, ktoré umožňujú potenciálny prístup útočníkovi do jeho počítača. Pri samotnom použití stránky sa zrejme klient nemohol vyhnúť podvodu tým, že by si v ľavom hornom rohu prehliadača overil certifikát banky. Aj tento bezpečnostný prvok totiž útok mohol simulovať. Kritické je však, že klient sa stále mohol vyhnúť útoku tým, že by na základe telefonického rozhovoru neoznámil údaje potrebné na autentifikáciu transakcie (SMS kód). Súd však zrejme nesprávne usúdil, že podstatná časť útoku sa odohrala pri nakazení počítača. Pričom opak je pravdou.

K získaniu SMS autentifikačného údaju podľa informácií VÚB došlo tak, že klientovi prišla SMS správa na potvrdenie žiadosti o zmenu telefónneho čísla v jeho online profile, a teda nie o potvrdení samotnej transakcie. Poskytnutím SMS kódu dokázal útočník následne zmenil pôvodné telefónne číslo klienta na svoje vlastné číslo. Klientovi tak už autorizačná SMS správa

na samotnú transakciu o prevode 3.000 eur nedošla vôbec, pretože bola zaslaná na iné telefónne číslo, ktoré bolo v moci útočníka[3].

Banka v takýchto prípadoch síce dokáže vystopovať účet, na ktorý boli prostriedky prevedené, no zvyčajne patrí osobe, ktorá je tiež predmetom útoku, alebo len inej osobe, ktorá nemá s útokom nič spoločné. Spravidla sú prostriedky vybrané prostredníctvom bankomatov skôr, ako dokáže dotyčná banka niečo urobiť. Podľa bezpečnostného experta z Nethemba - Pavla Luptáka: "Jedine zavedenie silnej dvojfaktorovej autentifikácie akými sú napríklad hardvérové tokeny vo forme dôveryhodnej OTP kalkulačky (napríklad RSA token), softvérove tokeny vo forme dôveryhodnej smartphone aplikácie (napríklad Google Authenticator), prípadne špeciálne zašifrovanej SMS správy, by dokázala tento útok v prvej fáze odvrátiť."

2. ROZHODNUTIA

Prvostupňový súd (Okresný súd Trenčín, 8.3.2012, sp. zn. 21C/1432011) mal za to, že klient *nekonal* nedbanlivo, a preto banka musí niesť celú stratu sama. S tým sa nestotožnila banka, ktorá podala odvolanie argumentujúc, že:

> Súdu prvého stupňa vyčítal, že ignoroval tvrdenia banky o poučení každého klienta o bezpečnej práci s Internet bankingom, ktoré žalovaný na prihlasovacej stránke k internetovému bankovníctvu zverejňuje od roku 2008. Pri každom prihlásení sa tak navrhovateľ mal možnosť dôkladne oboznámiť s prezentovanými informáciami, najmä s dôrazným

[3] V skutočnosti je takýto útok možné zrealizovať troma spôsobmi. Tzv. „one time password“ (OTP) zaslané SMSkou je vždy v tomto scenári použité ako potvrdenie vykonania transakcie. Teoreticky sa teda prípad môže odohrať nasledovne: (i) Utočník má k dispozícii nástroje a disponuje potrebnými zručnosťami na získanie autorizačných údajov automatickým presmerovaním pôvodnej SMS na nové, podhodené telefónne číslo. V tom prípade by klientovi neprišla ani SMS s OTP, ani SMS o vykonanej transakcii; (ii) Klientovi prišla SMS o zmene telefónneho čísla v profile - a útočník OTP získa jej obsah od klienta telefonicky, použitím sociálneho inžinierstva. Útočník následne zmení pôvodné telefónne číslo klienta uvedené v profile na nejaké svoje, podhodené číslo. V tom prípade by už ale klientovi neprišla SMS o vykonanej transakcii. (iii) Útočník získa od klienta autorizačný údaj (či už SMS OTP, alebo pozíciu Grid karty) telefonicky, použitím sociálneho inžinierstva. Útočník následne v mene klienta zadá OTP pre validáciu pozmenenej transakcie. V tom prípade klientovi prišla SMS o vykonanej transakcii. Často sa však stáva, že klient si obsah SMS neprečíta podrobne, napr. si nevšimne číslo účtu prípadne ani sumu. Pozorným prečítaním SMS správy sa dá preto podvod v prípade (ii) a (iii) odhlaliť z jej textu, ktorý zvyčajne znie “ Zadanie prevodneho prikazu - Prijemca: ##########/#### - Suma: ##,## EUR - kod: ?????? platny do DD.MM.RRRR HH:MM:SS” (citované podľa informácií VÚB).

> upozornením, aby klienti neodpovedali na e-maily alebo telefonáty, v ktorých by ktokoľvek, vrátane osôb vydávajúcich sa za zamestnancov banky, žiadal o poskytnutie osobných informácií, čísel a zostatkov na účtoch alebo prístupových či autorizačných údajov. Takéto poučenie pre klientov je formulované veľmi jednoducho a zrozumiteľne a jeho súčasťou sú aj názorné ukážky a príklady obdobných útokov. Poukázal na to, že súd pojem bežný klient banky nekonkretizoval a neuviedol, na základe akého myšlienkového postupu dospel k záveru, že navrhovateľ spadá do tejto kategórie a prečo sa súd domnieva, že bežný klient banky sa nemusí zaťažovať čítaním upozornenia na prihlasovacej stránke do služby Internet banking. Len uviedol, že okrem upozornenia na prihlasovacej stránke zdôrazňuje banka potrebu zvýšenej bezpečnosti aj vo Všeobecných obchodných podmienkach k depozitným produktom a varuje klientov pred prezradením autentifikačných a bezpečnostných prvkov im neznámej osobe. Nakoľko navrhovateľ nevedel identifikovať osobu, ktorej počas telefonického hovoru prezradil dôverné údaje, označuje ju žalovaný ako navrhovateľovi neznámu osobu. Žalovaný sa domnieva, že práve vyjasnenie konania alebo nekonania navrhovateľa je potrebné na posúdenie alebo zodpovedanie otázky, či jeho správanie možno vyhodnotiť ako nedbanlivosť alebo nie. [..] **Vyslovil presvedčenie, že oznámenie bezpečnostných prvkov navrhovateľovi neznámej osobe možno považovať za porušenie obvyklej opatrnosti a teda za hrubú nedbanlivosť zo strany navrhovateľa**.

Odvolací súd (Krajský súd Trenčín, 19.06.2013, sp. zn. 17Co/213/2012, JUDr. Emília Zimová) sa plne stotožnil so súdom prvého stupňa, a teda s tým, že platiť má banka. Dôvodil tým, že:

> Z obsahu odvolania vyplýva, že žalovaný sa domáha aplikácie ust. § 12 ods. 2 zákona č. 492/2009 Z.z., s tým, že žalovaný ako platiteľ má znášať straty súvisiace s neautorizovanou platobnou operáciou, pretože bola zapríčinená splnením jednej alebo viacerých povinností podľa § 26 v dôsledku jeho hrubej nedbanlivosti.

Podľa § 26 citovaného zákona používateľ platobných služieb pri používaní platobného prostriedku je povinný:

a/ používať platobný prostriedok podľa podmienok upravujúcich vydávanie a používanie tohto platobného prostriedku,

b/ bez zbytočného odkladu oznámiť poskytovateľovi platobných služieb alebo osobe poverenej poskytovateľom platobných služieb stratu, odcudzenie, zneužitie alebo neautorizovanéo užitie platobného prostriedku,

c/ po získaní alebo prevzatí platobného prostriedku vykonať všetky primerané úkony na zabezpečenie ochrany personalizovaných bezpečnostných prvkov platobného prostriedku.

V prejednávanej veci je nepochybné, že žalobca ako používateľ platobných služieb splnil povinnosť, ktorá mu je uložená v ust. § 26 písm. b/, keď bez zbytočného odkladu oznámil žalobcovi neautorizované použitie platobného prostriedku. **Žalovaný považuje za okolnosť vylučujúcu jeho povinnosť podľa § 11 ods. 1 zákona 492/2009 Z.z. a vyplývajúcu z ust. § 12 ods. 2 zákona tú skutočnosť, že žalobca v súvislosti s vykonaním predmetnej platobnej operácie oznámil osobe, ktorá sa predstavila ako zamestnanec žalovaného, svoje identifikačné údaje**. **Uvádza však sám, že takéto konanie žalobcu možno považovať za porušenie obvyklej opatrnosti.**

Keď súd prvého stupňa túto okolnosť nepovažoval za hrubé porušenie povinnosti vyplývajúcej z ust. § 26 písm. a/ (používať platobný prostriedok podľa podmienok upravujúcich vydávanie a používanie tohto platobného prostriedku) a tým za nesplnenie povinnosti v dôsledku hrubej nedbanlivosti, s takýmto záverom sa stotožňuje aj odvolací súd, v dôsledku čoho považuje výklad a aplikáciu ust. § 12, významného pre právne posúdenie danej veci, za správny. Krajský súd preto rozsudok okresného súdu potvrdil.

Podľa tlačovej správy nebolo rozhodnutie Krajského súdu v Trenčíne ďalej možné napadnúť riadnymi opravnými prostriedkami, a preto ho VÚB rešpektovala a judikovanú sumu klientovi uhradila. VÚB však stále zvažuje, či využije inštitút mimoriadneho opravného prostriedku, poukazujúc na podľa jej názoru zásadné chyby v odôvodnení rozsudku. Zatiaľ však rozhodnutie napadnuté nebolo. Banka ďalej vo svojej tlačovej správe uvádza, že:

> "S výrokom a odôvodnením rozhodnutia sa však nestotožňujeme a považujeme ho za nesprávne. Máme za to, že súd dostatočne nevzal do úvahy viaceré z argumentov predložených zo strany VÚB, a.s. v konaní svedčiacich jednoznačne v prospech VÚB, a.s.. Jedná sa napríklad o hrubé nedbanlivostné konanie klienta pri ochrane jeho autorizačných prvkov. **V rozhodnutí sa totiž uvádza, že klient splnil povinnosť ktorú mu ukladá § 26 písm c) citovaného zákona že, používateľ platobných služieb pri používaní platobného prostriedku je povinný po získaní alebo prevzatí platobného prostriedku vykonať všetky primerané úkony na zabezpečenie ochrany personalizovaných bezpečnostných prvkov platobného prostriedku. To je však v príkrom rozpore so skutočnosťou, keďže klient nemal zabezpečenú konfiguráciu počítača tak, aby nemohlo dôjsť k jeho infiltrácii škodlivým kódom a taktiež vyzradil autorizačné prvky cudzím osobám. (To nie je povinnosťou ani možnosťou banky zabezpečiť v mene klienta)**. Pokial ide o daľšiu otázku týkajúcu sa iných prípadov, chceme zdôrazniť, že k jednotlivým prípadom, týkajúcim sa phishingu, je nevyhnutné pristupovať vždy výlučne individuálne a nemožno ich paušalizovať, nakoľko v každom z týchto prípadov sa, v zmysle ustanovení zákona č. 429/2009 Z.z. o platobných službách, vyhodnocuje predovšetkým konanie samotného klienta, a to najmä, akým podielom sám prispel k vykonaniu neoprávnenej platobnej operácie.“

3. KOMENTÁR

Tento prípad je zaujímavý hneď z niekoľkých uhlov pohľadu. V prvom rade, ak odhliadneme od právnických kulís sporu, je to *krásny prípad pre ekonomickú analýzu práva*. Prípad až sám ponúka otázku: kto by mal v takomto prípade niesť zodpovednosť za ukradnuté peniaze? Kto sa mohol najlacnejšie vyhnúť tejto strate? Ponúka ale aj zaujímavé spoločenské otázky: aký stav bezpečnosti si budeme takto vynucovať na internetových užívateľoch? Aké phishingové techniky by mal vedieť priemerný užívateľ odhaliť?

Prv si ale rozmeňme prípad na drobné (trošku zjednodušene). Napriek zdanlivému riešeniu právnej otázky v právnom predpise, zákony v skutočnosti diferenciáciou medzi situáciami ľahkej a hrubej nedbanlivosti, a teda tým či platí klient, banka alebo obidvaja v podstate určito nerieši. Podstatná rola je totiž ponechaná sudcovi, ktorý musí určiť, kedy užívateľ internet bankingu za konkrétnych okolností

- vedel, že môže byť vystavený podvodu, ale bez primeraných dôvodov sa spoliehal, že k tomu nedôjde (ľahká nedbanlivosť) alebo
- nevedel, že svojím konaním môže byť vystavený podvodu, hoci o tom vzhľadom na okolnosti a na svoje osobné pomery vedieť mal a mohol (hrubá nedbanlivosť).

Jeden spôsob ako sa pozrieť na situáciu je bežný právnický spôsob hľadania odpovede v lepších či horších argumentoch o tom, čo taká alebo onaká nedbanlivosť za daných okolností vlastne je. Iný, oveľa oslobodzujúcejší spôsob je priznať si, že nehľadáme odpoveď na otázku čo je, ale skôr *čo by mala byť* potrebná miera starostlivosti sledujúc cieľ maximalizácie spoločenského blahobytu.

Je dobré požadovať, aby banka niesla všetky náklady sama, ak preukázateľne zo svojej strany vyvinula veľké množstvo nákladov na to, aby sa vyhla týmto situáciám? Potrebujeme ju trestať a tým pádom ešte nejako motivovať, aby vynaložila viac nákladov na prevenciu? Je taká prevencia vôbec možná? Alebo naopak, máme žiadať, aby sa užívateľ lepšie staral o svoje technické prostriedky pre internet banking, a tým vynaložením pomerne nízkych nákladov (zvýšenej pozornosti) sa snažil

odhaliť phishing sám? Mali by sme ho motivovať k tomu, aby tak urobil, napríklad tým, že za okolností, kedy riziko rozpoznateľné a odstrániteľné bolo, bude musieť strpieť aspoň spoluúčasť? Alebo by sme ho mali vystaviť týmto požiadavkám pod hrozbou toho, že stratené peniaze sú úplne v jeho neprospech? Nebudeme tak ale motivovať zase banku k tomu, aby znížila svoju ostražitosť, keďže celé riziko presunieme na klientov? Toto všetko sú legitímne otázky, ktoré by si mal sudca položiť.

Užívateľ v tomto prípade síce pri vynaložení lepšej pozornosti zrejme *nemohol* odhaliť to, že stránka, na ktorú sa pripája, nie je skutočne pravou VÚB stránkou, mohol však lepšie zabezpečiť svoj počítať antivírusom alebo používať internetový prehliadač, ktorý netrpí známymi zraniteľnosťami. Do akej miery možno od konkrétneho klienta vyžadovať, aby tak urobil, ale bude závisieť aj od osoby klienta banky. O nej sa však nedozvieme z rozhodnutia nič. Je totiž predstaviteľné, že mladý klient banky dokáže svoj počítač takto zabezpečiť skôr a lacnejšie ako priemerný dôchodca. V každom prípade nemožno na užívateľov klásť privysoké nároky, keďže na vyhnutie sa mnohým vírusom by užívateľ musel byť častokrát bezpečnostný expert, alebo minimálne sledovať denne technologické správy, čo je isto nereálna predstava.

Oveľa podstatnejšia časť skutkového stavu, ktorá vypovedá o klientovej nedbanlivosti, je skôr telefonické oznámenie údajov tretej osobe, ktorá sa predstavila ako zamestnanec banky. Vzhľadom na to, že banky bežne robia osvetové kampane a poučujú svojich klientov o tom, že si nikdy nežiadajú údaje emailom alebo telefonicky, malo by u každého klienta banky pri takomto konaní tretej osoby zasvietiť červené svetlo. Ak totiž súdy začnú umožňovať, aby sa klienti zbavili svojej nedbanlivosti aj pri takto základnej podvodnej technike, znamená to, že banky budú zodpovedať takmer vždy. Navyše, bankám nebude daná žiadna možnosť brániť sa, keďže tento ľudský faktor žiadna autentifikácia nedokáže minimalizovať. Súdy by preto naopak ako KS Trenčín, mali vyžadovať všeobecne vysokú starostlivosť o bezpečnostné prvky pri komunikácií s tretími osobami či už telefonicky alebo mailom. Najmä ak neposkytovanie údajov takýmto spôsobov je v podstate štandardom nie len v bankovom sektore, ale aj celkovo na internete. Bohužiaľ zo skutkového stavu nie je možné zistiť ako prebiehal samotný telefonický rozhovor.

Pre porovnanie, nemecký Spolkový najvyšší súd nedávno rozhodol v spore (BGH, sp. zn. XI ZR 96/11)[4], kde sa klient banky domáhal náhrady podvodne prevedenej platby zo svojho účtu, ktorá bola umožnená tým, že podvodníkovi sám sprístupnil 10 autorizačných detailov zo svojej TAN karty (tabuľky). Klient banky napriek prechádzajúcim poučeniam zadal týchto 10 údajov, čím umožnil útočníkovi realizovať platbu. BGH bol názoru, že hoci vzhľad stránky nevykazoval žiadne podozrivé prvky, muselo byť klientovi zrejmé, že pri žiadosti o 10 údajov z TAN tabuľky sa musí jednať o podvod. A to aj preto, že banka predtým upozorňovala, že takéto informácie za žiadnych okolností od svojich klientov nežiada. Súd tak ustálil hrubú nedbanlivosť na strane klienta. Klient tak musel niesť celú stratu sám.

Je preto dôležité, aby banka svojich klientov intenzívne poučovala o tom ako možný podvod rozpoznať. Za istých okolností však môže byť banka v pozícií, že nedokáže urobiť viac, než urobila, pretože napríklad všetky kroky podvodníkov sa vykonávajú už mimo jej sféry vplyvu (pôsobenie na zákazníka, nakazenie jeho počítača a pod.). Banka by však stále mala mať podľa môjho názoru vnútorný systém (fraud management) ako indentifikovať podozrivé platby a tým predísť možným neautorizovaným platbám. Aj spomínaný nemecký prípad posudzoval, či sama banka mohla rozpoznať podozrivosť platby. V danom prípade to tak nebolo, pretože išlo o nízku platbu (5.000 eur) vykonanú v rámci EÚ, pričom útočník sa pohyboval v rámci nastaveného limitu klienta banky. Treba však povedať, že úspešnosť takéhoto vnútorného systému nemusí byť v konkrétnom prípade vysoká, keďže útočníci zvyčajne nerecyklujú účty, a tiež sa snažia vyhnúť akémukoľvek podozrivému správaniu.

Ak by ale banka mohla vykonať podstatné kroky ako by minimalizovala riziko aj mimo svojej sféry vplyvu, súd by si mal položiť otázku, či by nebolo rozumné banku motivovať, aby tieto kroky do budúcna podnikla. Zároveň by mal však súd uplatňovaním štandardu nedbanlivosti motivovať aj užívateľa internetového bankovníctva, aby sám dával väčší pozor (viď nižšie). Ak teda napríklad každá zo strán mohla vynaložiť pomerne nízke náklady, aby predišla tejto udalosti, motivovať by trebalo obidve strany. To

[4] Upozorniť ale treba, že BGH aplikoval nemecké právo na skutkový stav, pre ktorý ešte povinnosť eurokonformného výkladu neexistovala.

znamená prijať štandard ľahkej nedbalivosti na strane užívateľa, a teda tiež uložiť mu spoluúčasť.

Ak naopak banka nemohla urobiť takéto kroky, prinútiť ju k väčšej ostražitosti by znamenalo len zvýšiť riziko jej podnikania. A tým aj jeho cenu. Samozrejme banka by mohla toto riziko naďalej minimalizovať verejnej osvetou (reklamou), no zároveň by právo vôbec nemotivovalo užívateľa k tomu, aby si dával pozor. To by spôsobilo tzv. problém morálneho hazardu[5], kedy osoba, ktorá berie na seba risk, necíti jeho dôsledky, a preto ho neberie do úvahy pri svojom konaní. A to môže byť spoločensky neefektívne, keďže riziko aj tak niekto nakoniec zaplatí. Z tohto dôvodu musí štandard nedbanlivosti hroziť užívateľovi prípadne aj plnou stratou prostriedkov, nie len drobnou spoluúčasťou. Aby sme predišli tomu, že užívateľ za predpokladu maximálneho úsilia banky nevykoná nič sám, je dobré potrestať v takomto prípade užívateľa.

Po odstránení právnickej mágie, môže štandard ochrany bezpečnostných údajov preto vyzerať aj takto[6]:

a) **spoluúčasť** (ľahká nedbanlivosť), ak ako banka, tak aj užívateľ mohli urobiť viac, aby prešli podvodu,
b) **stratu nesie sám klient** (hrubá nedbanlivosť), ak banka vyvinula maximálne úsilie vo svojej sfére vplyvu, pričom užívateľ sa mohol lacno vyhnúť podvodu, no neurobil tak,
c) **stratu nesie sama banka** (diligentný užívateľ), ak banka vyvinula hoci aj maximálne úsilie, ale užívateľ použil všetky lacné spôsoby ako sa vyhnúť podvodu.

Z prípadu c) vidieť, že jasná preferencia pre riziko ostáva na banke, ktorá ho bude niesť aj ak lacné spôsoby prevencie, ktoré užívateľ mohol využiť síce boli využité, no k podvodu došlo napriek tomu. Pozorný čitateľ možno bude namietať, že takéto rozloženie nemusí vždy zodpovedať alokácii zodpovednosti podľa ekonomického princípu "cheapest cost avoider"[7]. A bude mať pravdu. Môže sa stať, že užívateľ by mohol vykonať aj drahšie kroky ako predísť podovodu u seba, pričom tieto by stále boli

[5] Pozri http://en.wikipedia.org/wiki/Moral_hazard

[6] Ako vidieť jeden zásadný odklon od bežného testovania nedbanlivosti spočíva v tom, že sa sústreďuje aj na správanie banky, nie len správanie klienta.

[7] GILLES, Stephen. Strict Liability, and the Cheapest Cost-Avoider. *Virginia Law Review*. 1992, roč. 78, č. 6, str. 1291-1375.

nižšie ako tie, ktoré by musela podniknúť banka a my by sme stále alokovali zodpovednosť u banky. Dôvod pre to však podľa plynie zo samotného § 12, ktoré riziko nealokuje nevyhnutne rovnomerne, ale asymetricky (ekonomická analýza samozrejme nemôže prepisovať zákon).

Ak by teda napríklad užívateľ mohol predísť konkrétnemu útoku len tým, že by si zakúpil úplne nový a drahý antivírus, hoci aj banka vykonala všetko rozumné na jej strane, súd by mal ustáliť, že stratu nesie banka (c). Naopak, ak by banka nedostatočne informovala svojho klienta o rizikách konkrétneho útoku, pričom sám klient mohol za vynaloženia lepšej pozornosti odhaliť, súd by mal ustáliť, že stratu nesú banka a klient. Vzhľadom na limitáciu zákona by sa klient podieľal len do výšky 100 eur (a). No a napokon, ak by banka dostatočne informovala svojho klienta o rizikách útoku, pričom ten by napriek tomu nevynaložil potrebnú pozornosť, aby sa útoku vyhol, súd by mal ustáliť, že stratu nesie výlučne sám klient banky (b). Treba pamätať na to, že banka vynaložením prostriedkov u seba (napr. osveta) častokrát predefinuje aj výšku nákladov, ktoré musí vynaložiť jej klient (napr. obozretnosť). Je teda v záujme banky, aby náklady pre klienta boli čo najnižšie, keďže inak môže niesť zodpovednosť častejšie ona. Vytvorením predpokladov pre nízke náklady na strane užívateľa dokáže banka v podstate preniesť časť rizika na klienta, čím predíde problému morálneho hazardu.

Domnievam sa, že v tomto prípade sa jedná práve o prípad, kedy by mal stratu niesť klient, nie banka. Banka totiž zjavne informovala klientov o tom, že od nich nikdy nežiada predmetné bezpečnostné údaje telefonicky. Preto hoci klienta nemuselo hneď diskvalifikovať samotné nainfikovanie počítača, jednoznačne by ho malo diskvalifikovať takéto oznámenie tretej osobe.

Ak by sme masovo nasledovali rozhodnutie KS Trenčín, veľmi ľahko sa môže stať, že klienti bánk nebudú mať žiadny záujem na ochrane ich vlastných bezpečnostných prvkov. Podobne ako poistenec, ktorý nie je vystavený žiadnej spoluúčasti môže inklinovať k preberaniu väčšieho rizika, pretože nemusí niesť jeho dôsledky. A keďže banka nedokáže zabrániť zraniteľnosti spôsobenej osobným vyzradením, znamenalo by to *de facto* automatickú zodpovednosť banky. Banka by mohla využiť len interné zmluvné spôsoby ako svojich klientov motivovať k lepšej bezpečnosti (napr.

vernostné odmeny a pod.), aby tak znížila svoje podnikateľské riziko. Tie by však nemuseli byť vždy dostatočne účinné, a tak by podnikateľské riziko musela prenášať na klienta vo výške zvýšenej ceny za svoje služby. Takto by boli v konečnom dôsledku na klientov prenášané náklady, ktorým sa mohli pôvodne vyhnúť sankcionovaním iba tých spotrebiteľov, ktorí nie sú ochotní vynaložiť náklady na lacné spôsoby prevencie (napr. zvýšenú pozornosť). Ako dôsledok by sa celý systém len neefektívne predražil pre spoločnosť.