Měšec.cz:

Analýza zabezpečení internetového bankovnictví v České republice

29. června 2005

Internetové bankovnictví je zřejmě nejdynamičtěji se rozvíjející oblastí českého finančního trhu. Využívají ho téměř 2 miliony klientů a ročně jejich počet roste o desítky procent. Klientům především umožňuje rychlou a pohodlnou správu finančních prostředků nezávisle na fyzické blízkosti a otevírací době banky. Vedle nesporných pozitiv však tento způsob komunikace obsahuje rizika, s nimiž je třeba počítat, aby je bylo možné minimalizovat. Tato rizika se týkají především zabezpečení účtu a prováděných transakcí proti zneužití třetí stranou.

Tématem této studie finančního serveru Měšec.cz je právě tento aspekt internetového bankovnictví. Studie podrobně mapuje aktuální situaci v České republice a přináší komplexní přehled toho, jaké jsou vlastnosti systémů jednotlivých finančních ústavů a jak se banky vyrovnávají s existencí potenciálních rizik, ohrožujících bezpečnost důvěrných dat.

Ze studie vyplývá, že základní verze zabezpečení internetového bankovnictví je v některých případech nedostatečná a dodatečné zabezpečení aplikace si banky často nechávají zaplatit. Je ovšem nutné zdůraznit, že samotná kvalita zabezpečení nestačí, pokud klient není dostatečně opatrný a při internetové komunikaci s bankou nedodržuje základní bezpečnostní pravidla. K tomu, aby se tato pravidla stala přirozenou součástí uživatelského chování, chce svým skromným dílem přispět i tato studie (ke studii je přiloženo Desatero bezpečného používání internetového bankovnictví).

Zabezpečení přenosu dat a identifikace banky

Přenos bankovních informací je velmi choulostivou záležitostí a jeho zabezpečení by měla být věnována náležitá pozornost. Problematiku zabezpečení můžeme rozdělit do tří kategorií: ověření identity banky, šifrování samotných dat a bezpečnost prohlížeče.

Ověření identity banky

Aby měl klient jistotu, že předává citlivá osobní data správnému subjektu, je potřeba zajistit nejen identifikaci zákazníka, ale také ověření totožnosti bankovního ústavu. V tomto případě je u všech bank shodně použit protokol SSL, kdy se banka prokáže webovému prohlížeči oficiálním SSL certifikátem, který obsahuje identifikační údaje potřebné k ověření totožnosti banky.

SSL certifikát je vydán některou z takzvaných certifikačních autorit, která zajišťuje důvěryhodnost certifikátu. Seznam těchto autorit je vložen v prohlížeči a ten jim implicitně důvěřuje. Seznam důvěryhodných certifikátů, které nelze ověřit, protože je nepodepsala žádná známá autorita, lze samozřejmě vlastními silami rozšiřovat. Je však potřeba k tomuto kroku přistupovat velmi obezřetně, abychom se vyhnuli podvrženým certifikátům, které by pak na falešném serveru mohly vytvořit dojem o jeho pravosti.

Samotné stažení certifikátu a jeho ověření má na starosti webový prohlížeč na klientském počítači. Ten se postará o všechny potřebné kroky a zajistí vše automaticky. V případě, že je ověření úspěšné a prohlížeč rozhodne, že certifikát je platný a klient tedy komunikuje se správnou bankou, spojení se bez jakéhokoliv upozornění naváže.

Šifrování dat

Pokud jsou bezpečně ověřeny obě komunikující strany, může klient vstoupit do systému internetového bankovnictví a začít s ním pracovat. Dalším slabým místem je v tomto případě cesta, po které putují data oběma směry. Kdokoliv má totiž možnost komunikaci zachytit, pozdržet, případně přečíst a pozměnit. To je pochopitelně naprosto nepřípustné. Proto je nutno data proudící oběma směry šifrovat.

Součástí SSL certifikátu je také veřejný šifrovací klíč, který je během úvodního představování předán klientovi. Ten na oplátku předá zpět svůj veřejný klíč. Od této chvíle je pak veškerá komunikace na straně odesílatele šifrována veřejným klíčem druhé strany.

Po přijetí jsou pak data opět dešifrována a následně normálně použita. O šifrování se opět stará transparentně webový prohlížeč a tuto činnost oznamuje obvykle ve stavové liště ikonou žlutého visacího zámku. Tím je uživateli oznamováno, že je vše v pořádku, SSL certifikát je platný a probíhá šifrování. Při kliknutí na tuto ikonu si pak můžeme přečíst informace z certifikátu a další údaje o komunikaci.

Všechny zkoumané banky používají dostatečně silné šifrování a SSL certifikáty vystavené u certifikačních autorit. V tomto směru je bezpečnost internetového bankovnictví zajištěna velmi dobře.

	Délka šifrovacího klíče	Podepsán autoritou
BAWAG Bank	128 bitů	VeriSign
Citibank	128 bitů	VeriSign
Česká spořitelna	128 bitů	VeriSign
ČSOB	128 bitů	První certifikační autorita
eBanka	128 bitů	VeriSign
GE Money Bank	128 bitů	VeriSign
HVB Bank	128 bitů	VeriSign
Komerční banka	128 bitů	VeriSign
Poštovní spořitelna	128 bitů	První certifikační autorita
Raiffeisenbank	128 bitů	VeriSign
Volksbank	256 bitů	VeriSign
WSPK	nezjištěno	VeriSign
Živnostenská banka	128 bitů	VeriSign

Bezpečnost prohlížeče

Na straně klienta je prohlížeč důležitou aplikací, jejíž bezpečnost je pro celou komunikaci naprosto klíčovou. Měli bychom se proto zabývat také jeho bezpečností. V každém případě musíme hledět na to, aby klientský počítač nebyl kompromitován a napaden špionážním softwarem.

To lze zajistit instalací kvalitních antivirových balíků a odstraňovačů spyware. Je také velmi žádoucí přistupovat k bankovní aplikaci jen z bezpečného počítače, ke kterému máme přístup jenom my.

Webový prohlížeč jako takový může být ohrožen zejména některou z bezpečnostních chyb, která vznikne během jeho vývoje. Ta může útočníkovi dovolit například podvrhnout certifikát nebo umožnit přesměrování části obsahu stránky na falešný server.

Těmto problémům se můžeme vyhnout jen sledováním bezpečnostních hlášení a včasným záplatováním. Udržování aktuální verze software by mělo být v případě počítače, na kterém provozujeme internetové bankovnictví, naprostou samozřejmostí.

Ne vždy je však možno chybu opravit. Na vině je většinou nedostupnost opravy, která ještě nebyla výrobcem dodána. Podívejme se tedy, jak jsou na tom nejpoužívanější prohlížeče:

Internet Info, s.r.o. Durychova 101, 142 00 Praha 4 Tel. 244 003 123, fax 241 003 220 www.mesec.cz www.iinfo.cz

Prohlížeč	Počet objevených chyb	Z toho nezáplatováno
Internet Explorer 6.x	82	31
Mozilla Firefox 1.x	19	7
Opera 8.x	5	0
Konqueror 3.x	10	1

Zdroj dat: Secunia, stav k 22. červnu 2005

Z pohledu množství chyb a rychlosti jejich oprav jsou na tom alternativní prohlížeče mnohem lépe než Internet Explorer. Chyb je celkově mnohem méně a jsou rychleji opravovány. Nové verze ostatních prohlížečů se objevují častěji než v případě Internet Exploreru. V případě, že aplikace internetového bankovnictví podporuje některý z těchto prohlížečů, měli byste jeho použití zvážit.

Zdaleka ne všechny chyby jsou kritické nebo nebezpečné přímo pro internetové bankovnictví. Počet chyb ale vypovídá o celkovém stavu prohlížeče a rychlosti jeho vývoje.

Autentizace klienta

Autentizace, neboli ověření totožnosti klienta, je další z klíčových oblastí zabezpečení internetového bankovnictví. Na základě autentizace má banka jistotu, že komunikuje se svým klientem a nikoli s osobou bez oprávnění k manipulaci s účtem.

Autentizaci klienta banky v České republice provádějí pomocí uživatelského jména a hesla, certifikátu, který může být případně umístěn na čipové kartě nebo tokenu, autentizačním kódem zasílaným na mobilní telefon nebo kódem generovaným autentizačním kalkulátorem. Šest z dvanácti bank nabízí svým klientům volbu způsobu přihlášení na účet.

Nejčastější možností, která je ale zároveň nejméně bezpečná a nejsnáze napadnutelná, je přihlášení uživatelským jménem a heslem. Tuto volbu nabízí devět bank, z nichž šest ji má jako jedinou alternativu. Nutno však podotknout, že většina z nich využívá jinou, bezpečnější metodu autorizace aktivních operací (viz dále).

Nejbezpečnější variantou je přístup pomocí kódu generovaného autentizačním kalkulátorem, který využívají tři banky (u HVB Bank je jedinou možností), dále autentizace kódem zasílaným SMS zprávou a certifikát uložený na čipové kartě.

Způsoby autentizace

	Uživ. jméno a heslo	Certifikát	Čipová karta	SMS kód	PIN kalkulátor
BAWAG Bank	ano				
Citibank	ano				
Česká spořitelna	ano		ano		ano
ČSOB	ano		ano		
eBanka		ano		ano	ano
GE Money Bank	ano	ano			
HVB Bank					ano
Komerční banka		ano	ano		
Poštovní spořitelna	ano				
Raiffeisenbank	ano				
Volksbank	ano				
WSPK	ano				
Živnostenská banka	ano	ano			

Zejména u autentizace uživatelským jménem a heslem je důležitá tvorba uživatelského jména a hesla. Jak jsou tvořena, ukazuje následující tabulka.

Internet Info, s.r.o. Durychova 101, 142 00 Praha 4 Tel. 244 003 123, fax 241 003 220 www.mesec.cz www.iinfo.cz

Tvorba uživatelského jména a hesla

	Uživatelské jméno	Heslo	
		Minimální délka	Musí obsahovat
BAWAG Bank	8 číslic	8 znaků	číslici, písmeno
Citibank	16 číslic (číslo karty)	8 číslic	číslice
Česká spořitelna	10 číslic	8 znaků	libovolná kombinace
ČSOB	8 číslic	5 číslic	číslice
GE Money Bank	číslo účtu	8 znaků	číslici, malé a velké písmeno
Poštovní spořitelna	8 číslic	5 číslic	číslice
Raiffeisenbank	8 číslic	8 znaků	číslici, písmeno
Volksbank	náhodné číslice a písmena (malá i velká)	8 znaků	číslici, písmeno
WSPK	4 znaky (volí klient)	6 znaků	libovolná kombinace
Živnostenská banka	5 číslic (volí klient)	8 znaků	číslici, písmeno

V případě, že klient zadá heslo chybně, má několik pokusů na opravu. Příliš velký počet pokusů na opravu zvyšuje šanci případného útočníka, ale pokud je počet pokusů příliš nízký, může naopak často docházet k nechtěnému zablokování přístupu k účtu.

Heslem, které je možné chybně zadat, není chráněn pouze vstup na účet, ale například přístup k čipové kartě, k autentizačnímu kalkulátoru apod. Níže uvedená tabulka shrnuje počet chybných pokusů o přihlášení před zablokováním aplikace nebo přístupu k účtu.

	Počet pokusů do zablokování přístupu k účtu
BAWAG Bank	5
Citibank	6
Česká spořitelna	3
ČSOB	3
eBanka	3/-*
GE Money Bank	3/5**
HVB Bank	-
Komerční banka	3/3***
Poštovní spořitelna	3
Raiffeisenbank	3 (4)****
Volksbank	6
WSPK	-
Živnostenská banka	3 (10)****

* *Zablokování bankovní aplikace nebo autentizačního kalkulátoru/certifikátu.*

** *Zablokování přístupu pomocí uživatelského jména a hesla/certifikátu.*

*** *Při vstupu na účet bez čipové karty se po třech pokusech jen zavře okno prohlížeče/čipová karta se zablokuje.*

**** *Počet chybně zadaných hesel po sobě (kumulovaný počet chybně zadaných hesel od poslední změny hesla).*

Nejméně chráněným internetovým bankovnictvím pomocí zablokování přístupu k účtu je WSPK, kde má potenciální útočník neomezené množství pokusů. K internetovému bankovnictví HVB Bank je heslo generováno autentizačním kalkulátorem. Po druhém chybném zadání hesla je navíc klient vyzván, aby další pokus opakoval po uplynutí jedné minuty, čímž se potenciální útok znesnadňuje.

Za povšimnutí stojí Raiffeisenbank a Živnostenská banka, které kromě zablokování přístupu k účtu při opakovaném chybném zadání hesla v po sobě jdoucích pokusech účet zablokují i v případě kumulovaného chybného zadání hesla.

Se zablokováním přístupu účtu souvisí způsob jeho odblokování. Vždy lze přístup odblokovat na pobočce, bohužel v mnoha případech je to jediná možnost, která může znepříjemnit například pobyt v zahraničí. Řada bank odblokuje přístup i telefonicky po ověření totožnosti klienta a BAWAG Bank umožňuje faxovou žádost.

	Způsob odblokování účtu
BAWAG Bank	faxová žádost (vrátí zpět původní heslo)
Citibank	telefonicky - ověření číslo karty, 2 čísla z 6 místného PINu, další otázka
Česká spořitelna	telefonicky - ověření číslo smlouvy nebo protokolu, vrátí původní heslo
ČSOB	na pobočce - při zablokování karty vystavení nové
eBanka	na pobočce - při zablokování autentizačního kalkulátoru
GE Money Bank	na pobočce
HVB Bank	telefonicky - (při zablokování PIN kalkulátoru) 8:00 až 19:00, vrátí původní heslo
Komerční banka	na pobočce - při zablokování čipové karty
Poštovní spořitelna	na pobočce
Raiffeisenbank	telefonicky - 9:00 až 17:00, ověření osobního čísla; na pobočce
Volksbank	na pobočce
WSPK	-
Živnostenská banka	telefonicky - ověření 14místného SUK; na pobočce

Dojde-li k přihlášení k účtu, je dobré, má-li klient možnost se o této skutečnosti dozvědět např. SMS zprávou. Přestože banky hojně již nabízejí velmi flexibilní informační servis při změně stavu účtu, informaci o vstupu na účet se klient má možnost dozvědět jen u GE Money Bank a u Živnostenské banky. Cena 2,50 Kč za SMS u GE Money Bank a 1,90 Kč za SMS u Živnostenské banky je ale pro řadu klientů odrazujícím faktorem. Zaslání e-mailu je sice zdarma, ale zpráva o přístupu na účet zaslaná touto formou je mnohem méně praktická.

Alternativou k zasílání zpráv je informace o posledním (či posledních) přihlášení k aplikaci internetového bankovnictví, která odhalí potenciální vniknutí k informacím z účtu alespoň zpětně. Tuto možnost nabízí ČSOB a Poštovní spořitelna. Bohužel v informacích o přístupu je pouze datum a čas přihlášení, chybí např. IP adresa počítače, ze kterého se uživatel (nebo útočník) přihlásil.

Dalším důležitým bezpečnostním aspektem je čas, za který bude klient v nečinnosti od banky odhlášen. Pokud je doba příliš dlouhá, je větší nebezpečí zneužití při opuštění počítače bez odhlášení. Je-li ale příliš krátká, může být překážkou v plynulé práci.

	Doba do automatického odhlášení klienta
BAWAG Bank	5 min.
Citibank	5 min.
Česká spořitelna	max. 20 min.
ČSOB	20 min.
eBanka	není
GE Money Bank	5 min.
HVB Bank	5 min.
Komerční banka	5 min.
Poštovní spořitelna	20 min.
Raiffeisenbank	není
Volksbank	30 min.
WSPK	30 min.
Živnostenská banka	30 min.

V případě, že klient není odhlášen, může nepovolaná osoba přístupu využít k získání citlivých dat o stavu účtu, transakcí a jiných pasivních informací. Nejdelší čas má k dispozici u eBanky a Raiffeisenbank, kde k automatickému odhlášení nedojde vůbec.

Umožnění pasivních operací při neodhlášení uživatele v nečinnosti nemusí nutně znamenat nebezpečí převedení peněz na jiný účet. Aby mohl útočník platbu provést, musí obejít ještě jeden bezpečnostní mechanismus a platbu autorizovat.

Autorizace platby

Autorizace platby (ověření pokynu) probíhá ve většině případech stejným prostředkem, jako autentizace klienta. Většina bank, které při autentizaci klienta vyžadují pouze uživatelské jméno a heslo, pro autorizaci plateb využívají navíc podpisový certifikát. Jen v případě Citibank, České spořitelny a GE Money Bank (zde se to týká internetového bankovnictví Genius při použití uživatelského jména a hesla) není platba již dodatečně autorizována. Jedná se o velmi závažnou bezpečnostní chybu, navzdory krátkému času do odhlášení při nečinnosti klienta (5 minut, viz výše).

Způsob autorizace aktivních operací shrnuje následující tabulka:

	Autorizace transakcí			
	Certifikát	Čipová karta	SMS kód	PIN kalkulátor
BAWAG Bank	ano			
Citibank				
Česká spořitelna		ano		ano
ČSOB		ano	ano	
eBanka	ano		ano	ano
GE Money Bank	ano			
HVB Bank				ano
Komerční banka	ano	ano		
Poštovní spořitelna			ano	
Raiffeisenbank	ano			
Volksbank	ano			
WSPK	ano**			
Živnostenská banka	ano		*	

* *Živnostenská banka nabízí autorizaci pomocí jednorázových hesel TAN. Jednorázové heslo je možné zaslat SMS zprávou (v ceně 1,90 Kč/SMS).*

** *Certifikát lze uložit na USB token iKey, čímž je zvýšena bezpečnost.*

Všechny banky, které využívají autorizaci plateb (tj. všechny kromě Citibank, České spořitelny a GE Money Bank v případě základní autentizace klienta při vstupu na účet uživatelským jménem a heslem) při odesílání platby vyžadují dodatečnou autentizaci klienta v podobě zadání hesla k podpisovému certifikátu (či certifikátu na čipové kartě) nebo BPINu při žádosti o autorizační kód na mobilní telefon. Výjimkou je Poštovní spořitelna, která platbu autorizuje kódem zaslaným nešifrovanou SMS zprávou, k němuž je přístup i bez dodatečné autentizace (obdobně Živnostenská banka při zaslání jednorázového hesla TAN SMS zprávou).

Kromě autorizace platby jsou prostředky na účtu chráněny denními limity transakcí, které lze ve všech bankách nastavit a které mají některé banky povinně nastavené. Např. Citibank má standardní denní limit transakcí stanoven na 125 tis. Kč, Česká spořitelna na 50 tis. Kč, který lze zvýšit na 100 tis. Kč a který lze překročit pouze s vyšším stupněm zabezpečení, GE Money Bank pro verzi internetového bankovnictví se vstupem pomocí uživatelského jména a hesla jen 10 tis. Kč a Poštovní spořitelna standardně 50 tis. Kč s možností zvýšení na 300 tis. Kč.

GE Money Bank dle svých slov užívá monitorovací systém, který pomáhá odhalit podezřelé transakce, ale který blíže nespecifikovala z bezpečnostních důvodů.

Bezpečnostním mechanizmem, chránícím klienta před vyprázdněním účtu, je nastavitelné zasílání zpráv při změně zůstatku na účtu. Není sice stoprocentní (zpravidla lze změnit nebo zrušit přímo v aplikaci s použitím stejných prostředků autorizace jako u platby), ale jistý přínos nepochybně má. Zasílání zpráv nabízejí Česká spořitelna, ČSOB, eBanka, GE Money Bank, Komerční banka, Raiffeisenbank a Živnostenská banka.

Kolik stojí zabezpečení

Vyšší úroveň zabezpečení s sebou nese vyšší náklady. Ty banky často přenášejí na své klienty, čímž je mnohdy odrazují od využívání bezpečnějších technologií.

Určení ceny internetového bankovnictví a jeho zabezpečení není zdaleka triviální problém. Některé banky zahrnují cenu zabezpečení do měsíčního poplatku za službu, jiné si nechávají vyšší úroveň zabezpečení připlatit a u mnohých je vedení internetového bankovnictví zahrnuto v různých "balíčcích" účtů a přímého bankovnictví. Proto se zaměříme především na pořizovací náklady zabezpečovacích technologií (certifikáty, čipová karta, PIN kalkulátor) a na cenové rozdíly mezi jednotlivými variantami autentizace a autorizace v rámci každé bankovní aplikace.

Pro orientaci uvádíme cenu za vedení internetového bankovnictví:

	Zřízení	Vedení
BAWAG Bank	0 Kč	30 Kč
Citibank	0 Kč	0 Kč
Česká spořitelna	0 Kč	25 Kč*
ČSOB	0 Kč	20 Kč
eBanka	0 Kč	0 Kč**
GE Money Bank	0 Kč	39 Kč
HVB Bank	490 Kč***	50 Kč
Komerční banka	0 Kč	44 Kč
Poštovní spořitelna	0 Kč	0 Kč
Raiffeisenbank	0 Kč	35 Kč
Volksbank	0 Kč	30 Kč
WSPK	0 Kč	0 Kč
Živnostenská banka	0 Kč	30 Kč

** Sporožiro, sleva na vedení účtu 20 Kč, zahrnuje i telefonní bankovnictví.*

*** Programy "Zdarma".*

**** Zřízení a inicializace PIN kalkulátoru.*

Většina bank si neúčtuje žádné poplatky za zřízení internetového bankovnictví. Za výjimku lze považovat HVB Bank, která nabízí jedinou variantu zabezpečení, k níž klient musí pořídit autentizační kalkulátor. U ostatních bank jsou vstupními náklady zpoplatněny jen vyšší úrovně zabezpečení internetového bankovnictví.

	Nadstandardní zabezpečení (aktivace/zřízení)	
	PIN kalkulátor	Čipová karta + čtečka
BAWAG Bank	-	-
Citibank	-	-
Česká spořitelna	1 350 Kč	990 Kč
ČSOB	-	600 Kč
eBanka	89 Kč/měsíc	-
GE Money Bank	-	-
HVB Bank	-	-
Komerční banka	-	1 247 Kč
Poštovní spořitelna	-	-
Raiffeisenbank	-	-
Volksbank	-	-
WSPK	-	2000 Kč*
Živnostenská banka	-	-

** Umístění certifikátů v USB tokenu iKey.*

Banky nevyžadují, aby byly výhradními dodavateli čteček čipových karet, takže klienti je mohou zakoupit i jinde. Přesto při zřizování zabezpečení čipovou kartou bývá právě banka nejčastějším dodavatelem čteček k internetovému bankovnictví, a proto uvádíme cenu včetně základní verze čtečky čipové karty.

Nejvíce limitující je cena nadstandardního zabezpečení u České spořitelny, kde je základní varianta přihlášení k účtu uživatelským jménem a heslem a kde není při zadávání aktivních příkazů účet jištěn dodatečnou autentizací klienta. Bezpečnosti aplikace je tedy nedostatečná.

U bank, které využívají podpisové certifikáty, je důležitou informací cena za obnovu certifikátu. V naprosté většině případů vygenerování nových certifikátů není zpoplatněno, výjimku tvoří Česká spořitelna, ČSOB a eBanka, které ale nabízejí i jiný způsob autentizace klienta a autorizace příkazů.

	Obnova certifikátu
BAWAG Bank	0 Kč
Citibank	-
Česká spořitelna	320 Kč
ČSOB	200 Kč*
eBanka	200 Kč
GE Money Bank	0 Kč
HVB Bank	-
Komerční banka	0 Kč
Poštovní spořitelna	-
Raiffeisenbank	0 Kč
Volksbank	0 Kč
WSPK	0 Kč
Živnostenská banka	0 Kč

** 100 Kč roční obnova certifikátu plus 300 Kč tříletá obnova čipové karty.*

V neposlední řadě jsou zpoplatněny zprávy zasílané z banky klientovi, např. při změně stavu účtu. Čím vyšší je zpoplatnění, tím nižší je motivace klientů k jejich využívání.

	Zaslání zpráv			
	e-mail	fax	dopis	SMS
BAWAG Bank	-	-	-	-
Citibank	-	-	-	-
Česká spořitelna	0 Kč	10 Kč	15 Kč + poštovné	0 Kč
ČSOB	1 Kč	-	-	2 Kč
eBanka	2,90 Kč/3,90 Kč*	22,90 Kč/23,90 Kč*	22,90 Kč/23,90 Kč*	2,90 Kč/3,90 Kč*
GE Money Bank	-	6 Kč	-	2,50 Kč
HVB Bank	-	-	-	-
Komerční banka	0 Kč	5 Kč	-	1 Kč
Poštovní spořitelna	0 Kč	-	-	3 Kč
Raiffeisenbank	-	50 Kč	50 Kč	3 Kč
Volksbank	-	-	-	-
WSPK	-	-	-	-
Živnostenská banka	0 Kč	5 Kč	-	1,90 Kč

** Program Plus/Základ.*

Závěr

Základní verze zabezpečení internetového bankovnictví bývají mnohdy nedostatečné, což je nejvíce vidět v případě internetového bankovnictví Citibank a České spořitelny. Dodatečné zabezpečení aplikace si banky často nechávají zaplatit, přičemž zářným příkladem je opět aplikace České spořitelny, u níž je ekonomické zvýhodnění nezabezpečeného přístupu k účtu nejvíce zřetelné. Citibank zvýšení zabezpečení vstupu na účet nenabízí ani s příplatkem...

WSPK je také bankou, která významným způsobem motivuje klienty k využívání nižší úrovně zabezpečení ekonomickým stimulem, ovšem v základní verzi na rozdíl od Citibank a České spořitelny užívá alespoň klasický podpisový certifikát při autorizaci platby.

Mezi banky s nejlepším zabezpečením vstupu na účet v základní verzi (tj. bez doplatků) patří eBanka (šifrovaná SMS zpráva pomocí SIM Toolkit) a HVB Bank (autentizační kalkulátor). Klienti si mohou za velmi kvalitní zabezpečení připlatit u České spořitelny (certifikát na čipové kartě a autentizační kalkulátor), ČSOB a Komerční banky (certifikáty na čipových kartách).

Vstup na účet je nejméně chráněn (a klient si nemůže ani zvolit vyšší úroveň zabezpečení) u BAWAG Bank, Citibank, Poštovní spořitelny, Raiffeisenbank, Volksbank a WSPK.

O něco lépe jsou chráněny aktivní operace. I zde jsou ale banky, které ověření transakcí nevyžadují - Citibank a Česká spořitelna. Aktivní operace nejlépe chrání stejné banky, které chrání nejlépe i vstup na účet, klienti si mohou kvalitnější autorizaci připlatit také u WSPK (certifikát na USB tokenu), Živnostenské banky (jednorázová hesla TAN) a Poštovní spořitelny (SMS kód).

Ať je ale internetové bankovnictví zabezpečeno sebelépe, bez dodržování základních pravidel bezpečnosti ze strany klientů se neobejde. Nerespektování základních pravidel bezpečnosti, uživatelské chyby a vyzrazení přístupu k účtu jsou nejčastější příčinou zneužití internetového bankovnictví (v příloze č.2 je k dispozici **Desatero bezpečného používání internetového bankovnictví**).

Příloha č.1: NEJ internetového bankovnictví

Nejdelší šifrovací klíč
- Volksbank (256 bitů)

Největší počet možností autentizace klienta
- eBanka, Česká spořitelna (3 způsoby)

Největší počet možností autorizace platby
- eBanka (3 způsoby), Česká spořitelna (2 způsoby + "žádná")

Nejdelší povinné uživatelské jméno
- Citibank (16 znaků - číslo platební karty)

Nejrychlejší informace o neoprávněném vstupu na účet
- GE Money Bank, Živnostenská banka (volitelné SMS info při vstupu na účet)

Nejdelší doba odhlášení od účtu
- eBanka, Raiffeisenbank (nikdy nedojde k automatickému odhlášení)

Nejnižší maximální denní limit transakcí
- GE Money Bank (10 tis. Kč u aplikace s nižší úrovní zabezpečení)

Nejvyšší minimální poplatek při zřízení internetového bankovnictví
- HVB Bank (490 Kč - platí se za autentizační kalkulátor)

Nejvyšší cena za nadstandardní zabezpečení
- WSPK (2 000 Kč za umístění certifikátů v USB tokenu)

Nejdražší roční obnova podpisového certifikátu
- Česká spořitelna (320 Kč)

Nejlevnější SMS zprávy při změně stavu účtu
- Česká spořitelna (0 Kč)

Internet Info, s.r.o. Durychova 101, 142 00 Praha 4 Tel. 244 003 123, fax 241 003 220 www.mesec.cz www.iinfo.cz

Příloha č.2: Desatero bezpečného používání internetového bankovnictví

1. Neprozrazujte přístupové kódy a hesla k účtu blízkým osobám ani pracovníkům banky.

2. Nezaznamenávejte si přístupové kódy a hesla k účtu. Pokud jste k tomu nuceni např. složitostí uživatelského jména a délkou hesla, snažte se je zaznamenat způsobem, který nenapoví případnému nálezci kódů, že se jedná o přístup k internetovému bankovnictví. Zároveň uchovávejte přístupové údaje (např. uživatelské jméno a heslo) odděleně.

3. Pravidelně měňte užívaná hesla.

4. Vyhýbejte se užití neznámých počítačů např. v internetových kavárnách, zvláště pokud nepoužíváte jednorázová hesla pro vstup na účet. V případě, že neznámý počítač musíte využít, při nejbližší následné příležitosti změňte heslo.

5. Pravidelně aktualizujte internetový prohlížeč a operační systém.

6. Využívejte a pravidelně aktualizujte antivirové programy.

7. Podpisový certifikát neukládejte na pevný disk ani na internet.

8. Nedůvěřujte e-mailům z banky, které jste si neobjednali. Nikdy své bezpečnostní údaje neposílejte e-mailem.

9. Ověřte si certifikát stránky, na které se k účtu přihlašujete. Pokud se vám přihlášení k účtu nepodaří, přestože vkládáte dle vašeho názoru správné uživatelské jméno a heslo, neprodleně kontaktujte banku - mohli jste být přesměrováni na jiné stránky.

10. Při ukončení práce s internetovým bankovnictvím se vždy odhlaste a zavřete okno prohlížeče.

Autoři studie:

Petr Zámečník, zamecnik@iinfo.cz
šéfredaktor finančního serveru Měšec.cz
Tel. 244 003 127, fax 241 003 220
www.mesec.cz

Petr Krčmář, krcmar@iinfo.cz
šéfredaktor serveru Root.cz
www.root.cz