Čtyři stupně přístupu do banky

Přístup do banky není vhodné podceňovat. I když se jedná o jedny z **NEJZABEZPEČENĚJŠÍCH SYSTÉMŮ**, hackeři stále zdokonalují své útoky. Ukážeme vám, jak přistupovat do banky opravdu bezpečně.

VRATISLAV KLEGA

Tisková zpráva Komerční banky: *KB důrazně odmítá dnes zveřejněnou informaci o zneužití vnitřních systémů banky. Vnitřní systémy banky nebyly v žádném případě narušeny. Komerční banka zaznamenala 10 případů klientů, u kterých se objevily pokusy o zneužití jejich osobních počítačů. Pro další posílení bezpečnosti při využívání počítače klienta pro komunikaci s bankou je nutné rovněž dbát na dodržování bezpečnostních pravidel.* Zdroj: **www.kb.cz/cs/com/press/news/264.shtml**.

Komerční banka má pravdu – vnitřní systémy zneužity nebyly. Jenže klientům někdo ukradl přístupové certifikáty a také hesla. Zloděj tak mohl neomezeně manipulovat s prostředky na účtu klienta.

Bezpečnost v bankách se od tohoto incidentu v mnohém zlepšila. I internetová mafie však zdokonaluje své způsoby, jak vysát peníze z účtů nebo platebních karet klientů bank. Obezřetnost je proto v každém případě namístě. Ukážeme vám, jak bezpečně přistupovat do banky.

1. stupeň: Zanedbatelné riziko

Pokud do banky přistupujete ze svého domácího počítače, na kterém máte záplatovaný operační systém, firewall, antivir a antispyware, a pokud nenavštěvujete nebezpečné internetové stránky a nespouštíte pochybné programy, nemusíte se při přístupu do banky bát. Pro hackera by bylo velmi obtížné obejít všechny ochrany a získat přístup k vašemu bankovnímu účtu. Do banky tedy můžete beze strachu.

2. stupeň: Malé riziko

Do banky se potřebujete přihlásit z práce nebo třeba z počítače kamaráda. Nic sice nenasvědčuje tomu, že by byl počítač napadený trojským koněm nebo přímo hackerem, opatrnost je ale vždycky namístě. Jak postupovat?

Především použijte svůj vlastní browser. Na Chip DVD najdete přenosnou verzi Opery. Tento prohlížeč zkopírujte na svůj USB flash disk a pro přístup do banky používejte výhradně tento prohlížeč. Výhodou Opery je, že je velmi málo rozšířená a útočníci se na ni nesoustřeďují. Proto je pro přístup do banky bezpečná.

Ještě než se ale do banky přihlásíte, proveďte kontrolu, zda není na počítači skrytě nainstalován keylogger. To je hackerský program, který neviditelně běží v systému a ukládá všechny stisky klávesnice, které provedete. Seznam stisknutých kláves poté odesílá svému majiteli, a ten tak vidí vše, co jste napsali – včetně hesel. Na Chip DVD najdete nástroj KL-Detector, který odhaluje, zda na počítači není keylogger nainstalován. Jak se program používá?

Soubor »KL-Detector.exe« zkopírujte z Chip DVD na svůj USB flash disk a na počítači, prostřednictvím něhož se budete chtít připojovat do banky, jej spusťte. Nejprve klikněte na »I Agree«, poté třikrát na »Next«. Nakonec se zobrazí návod, jak s programem pracovat. Klikněte na »OK«. Aplikace se minimalizuje ve formě otazníku do systémové lišty. Nyní je třeba, abyste zkusili napsat nějaký text. Proto spusťte poznámkový blok a začněte psát libovolný text. KL-Detector kontroluje, zda se znaky, které píšete, neukládají ještě někam jinam. Jakmile zjistí přítomnost keyloggeru, který znaky ukládá, ikona otazníku se změní na vykřičník. Chytré keyloggery však neukládají data stále, proto je třeba setrvat ve psaní aspoň několik minut. Dvojitým kliknutím na vykřičník zjistíte, do jakého souboru se stisky vašich kláves ukládají.

Co dělat, když keylogger najdete? Nejjednodušší radou je samozřejmě nepoužívat pro přístup zmíněný počítač. Pokud však potřebujete nutně do banky vstoupit, taková rada vám nepomůže.

Jednoduchým způsobem, jak keyloggery obejít, je využití virtuální klávesnice. Nástroj Free Virtual Keyboard, který na obrazovce počítače zobrazí standardní klávesnici, najdete na Chip DVD. Jeho použití je vel-

mi jednoduché: stačí spustit soubor »FreeVK.exe« a myší klikat na správná písmena nebo čísla. Keylogger tento způsob vstupu nerozpozná, a proto žádná hesla ani přístupy neuloží. A i když je na počítači červ, který snímá obrazovky, heslo nezjistí – místo hesla se zobrazí hvězdičky.

3. stupeň: Značné riziko

Počítač prošpikovaný spywarem většinou poznáte po prvních minutách práce na něm. Všechno je pomalé, v browseru vyskakují okna, běží na něm podivné procesy... Přistupovat z takového počítače do banky by bylo velmi nebezpečné. Určitě obsahuje spyware, který se jen třese na to, aby ukradl vaše hesla, čísla kreditních karet a vybílil vám účet. Jak bezpečně přistoupit z takového počítače k účtu? Virtuálně.

Většinou se jedná o počítač v internetové kavárně nebo v hotelu. Těžko proto na něj budete instalovat Virtual PC se svým bezpečným systémem. Tudy cesta nevede. Řešením je použití přenosné verze oblíbeného Microsoft Virtual PC. Samozřejmě nejde o oficiální verzi od Microsoftu, ale o speciálně upravenou verzi.

Předpokládáme, že máte nainstalovaný Microsoft Virtual PC 2007 a že v něm máte zprovozněný funkční operační systém, ideálně Windows XP SP3. Pokud Microsoft Virtual PC 2007 nainstalovaný nemáte, najdete jej na Chip DVD. Postup, jak do něj nainstalovat operační systém, jsme vám v Chipu již několikrát přinesli.

Dále na Chip DVD najděte složku, ve které je Virtual PC Portable. Celý obsah složky zkopírujte na svůj USB flash disk. Soubory nemají ani 4 MB, což je malá velikost, přesto doporučujeme použít USB flash disk aspoň o kapacitě 4 GB. Na takovém disku poběží XP bez problémů.

Bezpečný přístup: Z bankovního systému se dostanete bezpečně do banky. Problémem není ani certifikát nebo Java.

Z USB flash disku nyní spusťte soubor »PortableVirtualPC.exe«. Aplikace si přetáhne informace z nainstalovaného Virtual PC do své přenosné verze – bude to trvat přibližně minutu.

Dále je třeba, abyste přenesli svůj virtuální počítač z pevného disku na USB flash disk. Sice byste mohli na USB disk nainstalovat novou verzi systému, to by však bylo zbytečně pracné. Otevřete složku »Dokumenty\My Virtual Machines«. Zde uvidíte přehled virtuálních počítačů, které máte nainstalované. Vyberte tedy ten správný a zkopírujte soubor s koncovkou VMC. Jedná se o soubor, který popisuje vlastnosti virtuálního počítače. Vraťte se na USB disk a do složky »Virtual Machines« tento soubor vložte. Dále je třeba zkopírovat odpovídající pevný disk k tomuto virtuálnímu počítači. Pravděpodobně bude uložen přímo ve složce »Dokumenty«. Koncovka souboru je VHD. Poznáte jej i podle toho, že soubor má značnou velikost, minimálně bude mít 1 GB. Virtuální harddisk zkopírujte a opět jej vložte do složky »Virtual Machines« na USB flash disku.

Nyní vezměte USB disk a vyzkoušejte jej v jiném počítači. Stačí spustit »PortableVirtualPC.exe«, a zobrazí se známá konzole s výběrem virtuálního operačního systému. Vyberte systém, který chcete spustit, a klikněte na »Start«. Je pravděpodobné, že se zobrazí chybová hláška o chybějícím disku – ten jste totiž přesunuli do jiné složky. Stačí ale ukázat, že VHD soubor se nachází ve složce »Virtual Machines« na USB disku, a vše bude v pořádku.

UPOZORNĚNÍ: Microsoft Virtual PC 2007 je produkt, který má své sériové číslo, i když je distribuován zdarma. Přenesením na USB flash disk dojde také k přenesení sériového čísla. Dva virtuální stroje s jedním sériovým číslem však nemohou správně fungovat. Proto bude třeba po přenesení na USB flash disk Virtual PC z počítače odinstalovat a pak jej znovu nainstalovat. Odinstalací však přijdete o nastavení virtuálních počítačů. Proto doporučujeme složku »Dokumenty\My Virtual Machines« zazálohovat a po přeinstalování obnovit. Virtuální harddisky se po odinstalování nesmažou, těmi se tedy nemusíte zabývat.

Jaká je výhoda virtuálního počítače? Veškerý spyware zůstává na fyzickém počítači a k souborům, které máte uložené ve virtuálním počítači, se nijak nedostane. Tím je zcela eliminováno riziko, že by vám mohl být ukraden třeba přístupový certifikát nebo citlivé soubory. Pozor je třeba ovšem opět dávat na keyloggery. Ačkoliv pracujete ve zcela jiném systému, klávesnice je fyzicky připojena k počítači, který mů-

NAJDETE NA CHIP DVD

Bezpečné bankovnictví

Bankovní systém Chipu ► bezpečný operační systém
Free Virtual Keyboard ► virtuální klávesnice
KL-Detector ► detekuje keyloggery v systému
MS Virtual PC 2007 ► virtuální počítač
Virtual PC Portable ► přenosná verze virtuálního počítače
OperaUSB ► přenosná verze internetového prohlížeče

► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **BANKING**

PROBLÉMY

Bootování z USB

Některé starší počítače mají problém s bootováním z USB disků. Jak tento problém vyřešit?

Pokud počítač z vytvořeného USB disku nebootuje, zkuste nejprve zjistit, zda není problém v USB disku. Vyzkoušejte USB disk i na nových počítačích nebo na notebooku. Pokud se zde systém rozběhne, chyba bude v počítači.

Otevřete BIOS a hledejte položky, které souvisí s bootováním. BIOS někdy nabízí simulaci USB disků jako disket. Ideální je nastavit režim »USB Legacy Support«. Klidně vyzkoušejte všechny režimy, které BIOS pro bootování z USB nabízí, zde není co pokazit. Můžete vyzkoušet i více USB portů. Na našem testovacím počítači byl problém s bootováním z USB portů na přední části počítače, které byly pouze starého standardu USB 1.1, v zadních USB 2.0 portech fungovalo bootování bez problémů.

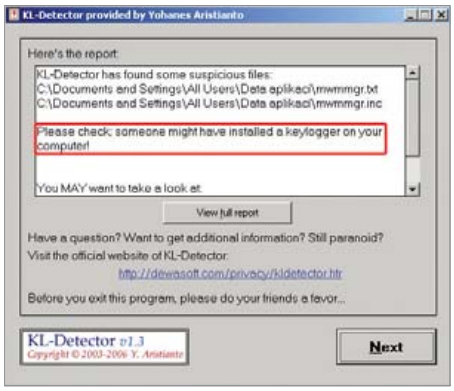
Pokud v žádném režimu bootování z USB disku nefunguje, bude nutné sáhnout po novém BIOS. Ten najdete na stránkách výrobce vaší základní desky. Nový BIOS problém s bootování téměř vždy vyřeší.

že být odposloucháván. Chcete-li přistupovat do banky zcela bezpečně a pokud to okolnosti umožňují, použijte nejtěžší kalibr – čtvrtý stupeň v podobě bankovního systému.

4. stupeň: Jakékoliv nebezpečí

Počítač již od pohledu vypadá jako žrout hesel? Báli byste se zde provést cokoliv? V takovém systému rozhodně nepracujte! Z kapsy vytáhněte svůj USB flash disk a počítač spusťte z něj. Přichystali jsme pro vás bezpečný operační systém, ze kterého budete moci přistupovat ke svému účtu, aniž byste měli strach, že někdo bude moci monitorovat váš účet, nebo z něj dokonce odčerpávat prostředky.

Bankovní systém je postaven na linuxové distribuci Slax, která patří mezi nejoblíbenější live distribuce, tedy operační systémy, které se spouští bez instalace. Takový systém si vystačí pouze se základním hardwarem, k běhu nepotřebuje třeba ani pevný disk v počítači. Na podobném systému bylo postaveno i záchranné Chip DVD, které jste mohli najít v Chipu 5/09. Tentokrát však sázíme na přenosné



Hledač keyloggerů: „Odposlouchává" někdo vaši klávesnici? KL-Detector to zjistí.

USB flash disky, ze kterých se systém spouští. To má několik výhod: na USB flash disku můžete mít uložen přístupový certifikát k bance, a pokud získáte nový, jednoduše jej nahradíte. Stejně tak můžete mít na USB disku další soubory, které budete potřebovat, třeba faktury ve formátu PDF, jež musíte zaplatit. Systém jsme optimalizovali pro co nejrychlejší spouštění a zároveň tak, aby na USB disku nezabral mnoho místa. Potřebuje pouze 228 MB, díky čemuž se vejde i na malý, 256 MB USB flash disk.

PŘÍPRAVA BOOTOVACÍHO DISKU: Na Chip DVD najdete soubor »banking.exe«. Jedná se o samorozbalovací archiv. Spusťte jej a obsah nechte rozpakovat přímo na USB flash disk. Soubory nesmí být v žádném adresáři, zadejte tedy přímo například »F:\«. Na flash disku mohou být jakékoliv jiné soubory, které budou v bankovním systému standardně přístupné. Jen je třeba, aby na disku bylo volných aspoň 256 MB.

Nyní je třeba zařídit, aby byl USB flash disk bootovací. Je proto třeba vytvořit na disku MBR (Master Boot Record), který zajistí, aby systém bootoval. Pro vytvoření MBR otevřete na USB disku adresář »boot« a spusťte soubor »bootinst.bat«. Soubor zjistí, na jakém disku je uložený, a na ten samý disk zapíše MBR. Průběžně o tom informuje průvodce.

UPOZORNĚNÍ: Ujistěte se, že soubor »bootinst.bat« opravdu spouštíte z USB flash disku. Pokud byste soubor spustili na systémové partition, přepíše MBR a po příštím restartu by se Windows nespustila.

SPOUŠTĚNÍ: Ke spuštění bankovního systému je třeba znovu spustit počítač a jako bootovací zařízení zvolit právě USB flash disk. Pro rychlé přepnutí bude stačit, pokud po spuštění budete na klávesnici mačkat klávesu [F8], dokud se nezobrazí výběr médií, ze kterých je možné bootovat. Zde pak stačí zvolit váš USB flash disk. Pokud rychlý výběr přes klávesu F8 nefunguje, bude nutné, abyste vešli přímo do BIOS a USB nastavit jako »First Boot Device«.

Pak se zobrazí menu s výběrem, co chcete spustit. Nejprve zvolte »Slax Graphics mode (KDE)«. Přibližně do dvou minut by se měl systém spustit a přivítá vás přehledné grafické rozhraní podobné Windows. Pokud však máte grafickou kartu, která s tímto systémem nefunguje, dočkáte se jen chybové hlášky. V tom případě restartujte počítač a zvolte čtvrtou možnost, »Slax Graphics VESA mode«. Tento mod je kompatibilnější a funguje prakticky se všemi grafickými kartami.

V nastartovaném systému pak zvolte »K | Internet | Firefox«. Spustí se známý prohlížeč, ze kterého můžete bezpečně přistupovat do banky. Součástí systému je i Java, takže nebudete mít potíže ani s takovým přístupem do banky, který Javu požaduje.

CERTIFIKÁT V SOUBORU: Chcete-li přistupovat k souborům, které máte na USB flash disku, je to velmi jednoduché. Stačí na ploše systému dvojitě kliknout na »Systém« a pak na »Úložná zařízení«. Zde vyberete svůj USB disk, na kterém uvidíte soubory, které jste sem nakopírovali ve Windows. Potřebujete-li při přístupu do banky certifikát, který je uložen na USB disku, postup je trochu složitější. Otevřete si stránku s přístupem do banky. Jakmile bude chtít prohlížeč cestu k certifikátu, zadejte cestu »\mnt\live\mnt«, a zde uvidíte připojené USB disky, například »sda1«. To už je přímý přístup k USB disku a najdete zde také svůj certifikát. Další postup je stejný jako ve Windows.

Výhodou je, že takto nikdo nezjistí vaše hesla, nemá vám jak ukrást certifikát, a díky tomu, že jsou přístupy do banky zabezpečené, nikdo vaši komunikaci ani neodposlechne.

ANONYMNĚ: V základní výbavě bankovního systému najdete i aplikaci Tork, což je anonymizační služba. Tork vás připojí k anonymizačnímu proxy serveru, který skryje vaši IP adresu a identitu. Live systém umocněný Torkem pak zaručí dokonalou internetovou anonymitu.

ŠIFROVÁNÍ: Máte na flash disku certifikát do banky, ale také třeba účetnictví, faktury nebo jiné důležité dokumenty? V tom případě byste neměli podceňovat šifrování. V bankovním systému najdete nástroj TrueCrypt, který slouží právě k šifrování souborů. Na vašem USB disku vytvoří šifrovaný soubor, který se bude do bankovního systému připojovat jako partition. Cokoliv na tuto partition uložíte, bude zašifrované a nikdo soubory bez znalosti hesla neuvidí.

VRATISLAV.KLEGA@CHIP.CZ