

Vážné bezpečnostní díry v produktech internetového bankovníctví

V konstrukci a provozu internetového bankovníctví bank, které jej provozují v České republice, byly nalezeny vážné slabiny, které ohrožují bezpečnost a důvěryhodnost těchto řešení!!

Jiří Nápravník se svým týmem našel v provozovaných aplikacích internetového bankovníctví Komerční banky, a.s., České spořitelny, a.s., Živnostenské banky, a.s., Raiffeisenbank, a.s. a CITI bank, a.s. bezpečnostní slabiny, které znehodnocují způsob identifikace uživatelů a ohrožují důvěryhodnost zmíněných aplikací.

Zdůvodnění :

Vlastní bezpečnost aplikací v síti internet je založena především na třech stavebních kamenech. Prvním je zabezpečení serveru, na kterém pracuje vlastní aplikace. Tuto oblast zabezpečují téměř všichni projektanti obchodních nebo bankovních systémů a pokud administrátoři věnují dostatečnou pozornost konfiguraci serverů, zprávám z IDS a auditním záznamům, je možné servery považovat za zabezpečené. V této oblasti jsme také slabiny nenašli.

Druhým stavebním kamenem je bezpečný komunikační kanál mezi bankou a klientem. Tento prvek byl ve zkoumaných řešeních internetového bankovníctví zajištěn na úrovni SSL a prolomení (rozluštění) tohoto zabezpečení by nepřineslo požadovaný efekt. Zjištěná slabina se netýká komunikačního kanálu mezi bankou a klientem.

Třetím stavebním kamenem, na kterém stojí bezpečnost internetového bankovníctví nebo obchodu, je spolehlivé a průkazné určení osoby a to při každém přihlášení. Ve způsobu realizace tohoto stavebního kamene byly nalezeny slabiny, které ohrožují spolehlivé a průkazné určení uživatele, který se ve skutečnosti přihlásil do aplikace internetového bankovníctví a provedl konkrétní operace.

Upřesnění :

Ve všech popisovaných případech se jedná o chybu v konstrukci a způsobu provozování aplikace. Nejde tedy o chybu v délce šifrovacího klíče nebo jinou chybu v použitých technologiích.

V případě České spořitelny, a.s. se jedná o odposlechnutí přihlašovacího jména a hesla. V případě Komerční banky, a.s., Živnostenské banky, a.s., Raiffeisenbank, a.s. se jedná o odposlechnutí přihlašovacího jména a hesla a současně zkopírování privátního klíče příslušného klienta.

V případě CITI bank, a.s. se jedná o odposlechnutí čísla karty, PIN kódu a zkopírování souboru pro generování hesla (Challenge – response).

Po získání uvedených náležitostí by se mohl případný útočník vydávat za oprávněného klienta a jeho jménem převést peníze. Oprávněný vlastník by to v lepším případě zjistil až po provedení operace nebo až na výpisu z účtu.

Přístup k výše uvedeným informacím, které jsou nutné pro přihlášení, pokud jsou na počítačích nebo disketách běžných uživatelů, není možné nijak spolehlivě ochránit proti zkopírování. Autorům této zprávy není ani znám způsob, jak přimět veterináře, architekty, obchodníky a další běžné uživatele výpočetní techniky, aby se účinně chránili proti stále novým a zákeřnějším útokům, které mají za cíl nepozorovaně se nainstalovat na počítač, shromažďovat důležité informace, které se na něm nacházejí a poslat je svému autorovi. Tuto úlohu by měl převzít ten kdo má vyšší odborné znalosti, tedy poskytovatel aplikace.

V současnosti se stále rozšiřují a zdokonalují počítačové viry a škodlivé kódy (spyware, adware), které se mohou na počítač běžného uživatele nainstalovat nepozorovaně při prohlížení některých www stránek nebo prostřednictvím elektronické pošty. Počítačové viry a spyware se v současnosti v mnoha případech „pouze“ šíří a neprovádí žádnou škodlivou činnost. To období může být (ale snad nebude) předzvěstí vážnějšího útoku, který bude cílen na klienty internetových bank a podobných aplikací a jehož cílem by bylo vážné ochromení těchto systémů a podlomení důvěry v moderní systémy komunikace a obchodování.

Přístup bank

Banky se ve svých obchodních podmínkách, které musí klient podepsat, zříkají veškeré odpovědnosti za škody způsobené při provozu internetového bankovníctví a doporučují klientům, aby si sami řešili bezpečnost prvků nutných pro přihlášení do konkrétního internetového bankovníctví. Jak jsme již uvedli výše v případě běžných uživatelů je to téměř nemožné a z našeho pohledu se jedná o nerovné podmínky. Banky mají své týmy specialistů na bezpečnost informačních systémů a provozují aplikaci s bezpečnostní slabinou, za což odmítají nést odpovědnost. Běžný uživatel neznalý rizik v prostředí počítačů a Internetu by se měl proti těmto nebezpečím účinně bránit. Je to podobně absurdní situace jako by výrobce automobilu řekl klientovi, že by si po každém sešlápnutí brzdového pedálu měl zkontrolovat kvalitu brzdové kapaliny a brzdové soustavy. Takový přístup je určitě absurdní. Nikdo si nedovolí chtít po advokátovi nebo veterináři, aby si kontroloval brzdy ve svém automobilu. Za konstrukci zodpovídá výrobce, který poskytuje i přesně danou záruku.

Hovořit ve vztahu s českými bankami o kyberterorismu bylo možná ještě před několika lety přehnané. Dnes jsou všechny banky, u kterých jsem slabinu v internetových bankovníctvích našel, součástí nadnárodních bankovních skupin a v tomto případě tato oblast dostává okamžitě jiný rozměr už proto, že je zvykem si z důvodu snižování nákladů na vývoj vyměňovat zkušenosti v rámci celého holdingu či skupiny firem. To znamená, že slabina, kterou jsem zjistil, ověřil a ve stručnosti popsal v této zprávě se může objevit i v dalších zemích, kde má konkrétní finanční skupina svoji pobočku.