Кражбите на самоличност и защитата на интернет банкирането

гл.ас. д-р Силвия Парушева
Икономически университет – Варна
e-mail: parusheva@ue-varna.bg

Резюме: В статията се разглежда един от актуалните проблеми за интернет банкирането към настоящия момент – кражбите на самоличност на потребителите и източване на пари от сметките им поради пропуски в начините за удостоверяването им от страна на банките. Представени са възможностите за решаването му чрез реализиране на проекти за многофакторна автентификация на банковите клиенти в съответствие с нивата на risk. Чрез сравняване на практиката в развитите страни (основно по примера на Великобритания) и тази в България са направени обобщения и препоръки за повишаване на сигурността на системите за онлайн банкиране.

Ключови думи: кражби на самоличност, фишинг, многофакторна автентификация, банкови чип карти, токън устройства.

JEL: C88, G21.

Електронните финансови услуги разширяват своето присъствие във всички области на финансовия пазар – банковата, застрахователната, търговията с ценни книжа и валута. Поради значителните си предимства те придобиват все по-голяма популярност сред потребителите. Доверието в тях обаче през последните няколко години е поставено на сериозно изпитание поради нарастващия брой на случаи на кражба на самоличност (идентичност) във все повече страни по света.

Кражбата на самоличност („**Identity theft**") може да се определи като злоупотреба с лични данни или документи с цел приемане на чужда самоличност и извършване на незаконни действия, като например злоупотреба с банкови или други активи на лицето. Особено засегнати са популярни типове банкови операции като транзакции с дебитни и кредитни карти на банкомати (ATM[1]) или POS[2] устройства (ПОС) и използване на банкови карти за плащания при електронната търговия в интернет. Тревожна тенденция в последно време е превръщането в обект на атаки на типичното онлайн банкиране – извършването на банкови операции по сметки на клиентите в средата на интернет.

Прието е мрежово базираните измами да се определят с понятието „фишинг" (**phishing**). Те представляват кражба на самоличност, при която чрез *фалшиви имейли* и *фалшиви интернет сайтове* се примамват наивни потребители да разкрият лична информация

[1] Automated Teller Machine
[2] Point-of-sale

като потребителски имена (User ID) и пароли, номера на кредитни карти и пинкодове, адреси, номера на банкови сметки и др. Най-често фалшивите имейли наподобяват имейли от самите банки и с линк предизвикват препращане към фалшифицирани уеб сайтове, идентични с банковите.

Друга разновидност на кражба на самоличност е свързана с използването на различни видове криминален софтуер, извършващ действия без знанието на потребителя. Към него се отнасят вируси от тип „троянски коне" (Trojans), червеи или програми от типа „keylogger", които се самоинсталират на компютъра на потребителя без негово знание. Те прихващат и записват въведените от клавиатурата пароли и други лични и финансови данни и ги изпращат към фишинг сървъри. Подобни престъпни действия се обозначават с понятието „**pharming**". Някои от тези вирусни технологии атакуват адресната лента на интернет браузъра и са по-усъвършенствани от phishing [9]. Когато потребителите въведат валиден URL[3] адрес, вместо към валидните сайтове те биват преадресирани към криминални уеб сайтове. Преадресирането към измамни сайтове се реализира чрез заразяване на локалния Domain Name Server (DNS). То включва промяна на специфичния запис за домейна, което води до изпращане на потребителя към сайт, различен от желания (очаквания).

Случаите на кражба на самоличност са най-разпространени в САЩ, Канада, Австралия и Южна Африка. В Европейския съюз проблемът е най-наболял във Великобритания. Използването на фишинг атаки датира от няколко години. Първите регистрирани атаки са през март 2003 г. Оттогава заплахите, основаващи се на вируси и червеи, нарастват бързо, а използването на „троянски коне" за незаконно придобиване на лична информация като сравнително нов феномен е регистрирано в криминалната практика след средата на 2004 г. [6].

По последни данни в *САЩ* през 2005 г. около 109 млн. компютърни потребители са подложени на фишинг e-mail атаки, което спрямо 2004 г. е нарастване със 100 %. Средният размер на стойността на измамите се е увеличил пет пъти в сравнение с 2004 г. [3]. Според изследване на Garthner[4] за една година (от средата на 2005 до средата на 2006 г.) 15 млн. американци са станали жертва на измами, свързани с кражба на самоличност, което представлява нарастване с приблизително 50 % спрямо оценките за 9,9 млн. измамени през 2003 г. [8].

Търговската асоциация на банките (APACS[5]) във *Великобритания* отчита, че загубите от фалшиви транзакции при онлайн банкиране през първата половина на 2006 г. са се увеличили с 55 % спрямо същия период на предходната година и са достигнали 22,5 млн. лири. За цялата 2006 г. измамите в резултат на интернет банкиране бележат ръст от 44 %, основно поради нарастването на фишинг атаките. По данни на CIFAS[6] от 2000 г. кражбите на самоличност за 5 години са се увеличили с 500 %. Според Федералната криминална служба в *Германия* през 2006 г. е имало 3500 реализирани фишинг атаки.

Публикувани са данни за сериозен ръст в използването на шпионски софтуер от типа „spy ware". Съгласно доклад, изнесен на конференция на Европейската комисия, броят на програмите „keylogger" е нараснал при-

[3] Universal Resource Locator
[4] http://www.id-protect.co.uk/fraud_statistics.php - Garthner Study 2007
[5] Association for Payment Clearing Services
[6] Асоциация във Великобритания, създадена във връзка с превенция на финансови измами.

близително 3 пъти през периода май 2005 – май 2006 г. [3]. Заедно с това броят на „keylogger distribution sites" – уеб сайтовете, които крадат пароли и разчитат на злонамерени кодове, за да получат лична финансова информация, се е увеличил с повече от 400 % за същия период.

Макар и непълни, цитираните по-горе данни показват обща тенденция за съществено нарастване на злоупотребите с лични данни при онлайн банкирането. Този факт в значителна степен застрашава дейността на банковите институции. Възможен е отлив на потребители на уеб базираните банкови услуги с всички произтичащи от това неблагоприятни последици.

Решаването на проблема може да се търси в няколко направления: сигурна автентификация на клиентите на банките, допълнителни законови гаранции, работа по информиране на потребителите, засилване на тяхната бдителност и отговорност и др.

В настоящата статия се изследват някои възможности за приложение на съвременните информационни технологии при осигуряване на надеждна автентификация на клиентите при интернет банкиране.

Начини за сигурна автентификация на потребителите при онлайн банкирането

Важни аспекти на сигурността на уеб банкирането са обезпечаване на защитен трансфер на данни между компютъра на клиента и банковите сървъри и надеждна автентификация на потребителите.

Проблемът с автентификацията е свързан с доказване на истинността на потребителя, потвърждаване на неговата действителна самоличност. Банките се затрудняват как със сигурност да установят дали онлайн банковите операции са наредени от истинския потребител, или от лице, присвоило личните му данни чрез шпионски софтуер.

За защита на трансфера на данни между банката и клиента при интернет банкирането се използват основно криптографски техники. Най-широко приложение намира протоколът „Secure Socket Layer" (SSL). Той криптира данните, с което осигурява тяхната защита при преноса им през интернет. SSL обаче не притежава средства за автентификация на потребителя, което налага използването на допълнителни техники.

Добри възможности предоставя протоколът „Secure Electronic Transaction" (SET), който позволява както криптиране на данните, така и надеждна автентификация на клиентите пред сървъра на системата. За съжаление твърде високата сложност и големите инсталационни и експлоатационни разходи са причина този протокол да не получи широко признание и разпространение.

Като се има предвид, че в банковата практика масово се използва протоколът SSL, възниква необходимостта от прилагане на допълнителни, при това надеждни средства за потвърждаване самоличността на клиента.

Известни са три основни начина за автентификация – нещо, което потребителят *знае* (*knowledge* – парола, ПИН); нещо, което потребителят *притежава* (*possession* – банкова чип карта, хардуерни устройства, т.нар. „secure tokens"); нещо, което потребителят *представлява* – специфична физическа, т.е. биометрична особеност (пръстов отпечатък, сканиране на ириса, ретината и др.) [1, с. 48].

Всеки от трите начина има своите предимства и недостатъци, при това недостатъците съответно се използват като възможности за преднамерена криминална намеса и пробиви в сигурността. Това е причината финансовата индустрия да се ориентира към комбиниране на начините за автентификация на клиентите, в резултат на което в практиката вече се прилага **многофакторна автентификация** в различни разновидности – двуфакторна, трифакторна и т.н.

Двуфакторната автентификация включва освен използването на потребителски имена и пароли (ID/password), т.е. „нещо, което потребителят знае", и приложение на още един фактор, най-често от типа „нещо, което потребителят има", като например **хардуерни устройства за сигурност**, наричани „**токъни"**. Различават се най-общо 3 типа устройства – *USB токъни*, *смарт карти и четци на смарт карти* и *токъни, генериращи пароли* [4, с. 8].

USB токън устройството се поставя в USB порта на клиентския компютър, поради което не се изисква инсталиране на специален хардуер. След автоматичното разпознаване на токъна потребителят трябва да въведе паролата като втори автентификационен фактор, за да получи достъп до компютърната система. Освен това устройството има възможности да съхранява цифрови сертификати, които могат да бъдат използвани в PKI[7] инфраструктурата.

Смарт картата съдържа микропроцесор, който може да съхранява и обработва данни. Включването на микропроцесора позволява на софтуерните разработчици да използват по-силна схема на автентикация. Приложението на смарт картата изисква съответен четец, свързан с клиентския компютър. Ако смарт картата бъде разпозната за валидна (първи фактор), потребителят трябва да въведе парола (втори фактор), за да завърши автентификационният процес.

И двете устройства са трудни за възпроизвеждане и фалшифициране, и по този начин са по-сигурно средство за съхраняване на чувствителни данни. Основният недостатък на смарт картите като средство за автентификация е, че изискват инсталация на хардуерен четец и придружаващи софтуерни драйвъри на клиентския компютър. Предимство на USB токън устройството е облекчената експлоатация, тъй като не е необходимо инсталиране на специален хардуер.

Токънът, генериращ пароли, създава уникални пароли, известни като еднократни пароли (one-time passwords /OTPs/), всеки път, когато се използва. Те се изобразяват на малък екран на токъна и продължителността на живота им е от 30 до 60 секунди. Потребителят първо въвежда потребителското си име и обичайна парола (първи фактор), следвана от еднократната парола, генерирана от токъна (втори фактор). Този тип устройства са значително по-сигурни поради времевите ограничения за валидност на паролата, а също и поради факта, че няма физически контакт между устройството и компютъра (токънът се захранва с батерии). Случайността, непредсказуемостта и уникалността, както и кратката продължителност на живот на паролите гарантират, че евентуалното им прихващане от програми „keylogger" не представлява опасност за потребителите.

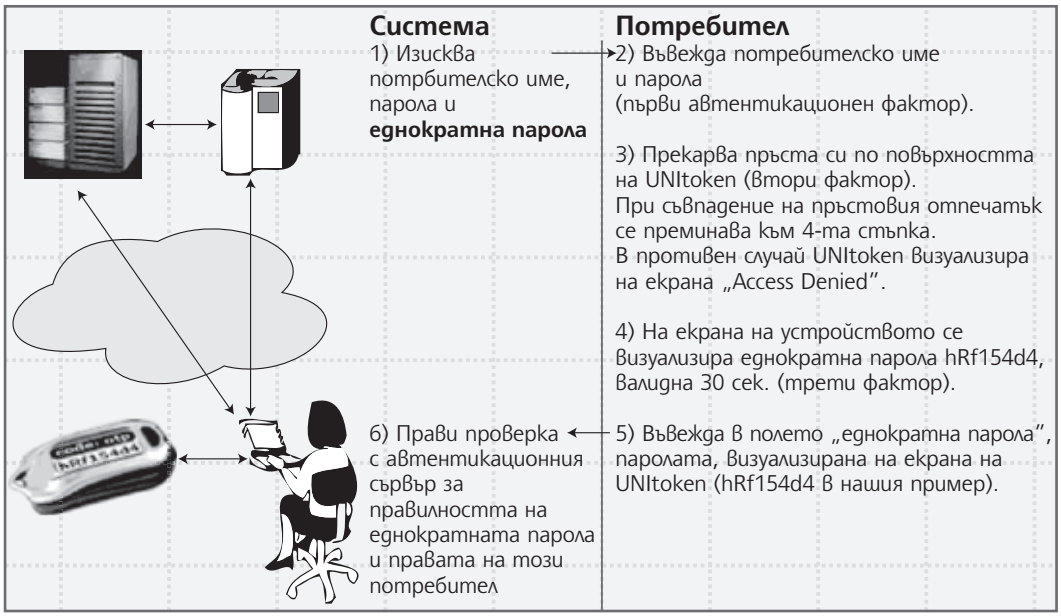
Друг вариант на автентификационен признак при двуфакторната автентификация е **методът на „поделените тайни"**. Поделените тайни („нещо, което потреби-

[7] Public Key Infrastructure

телят знае") са информационни елементи, които се знаят или поделят и от двете страни – клиента и автентифициращата институция. Към по-новите представители на техниката на поделените тайни принадлежат *въпроси*, които изискват специфично потребителско знание като техен отговор или избрано от потребителя *изображение*, което трябва да бъде селектирано от серия предложени изображения. Сигурността на поделените тайни може да бъде увеличена с изискване за периодична смяна, тъй като при „статичните тайни" (тези, които никога не се сменят) рискът от компрометиране се увеличава с времето. Използването на няколко поделени тайни също осигурява нарастваща сигурност.

Двуфакторната автентификация може да се превърне в **трифакторна,** когато към нея се включи и **биометрично разпознаване**. В представената на фигура 1 автентификационна процедура е включено устройство token с вградено разпознаване на пръстови отпечатъци, при което проверката на пръстовия отпечатък е втори фактор, а въвеждането на еднократна парола е трети фактор. По този начин се реализира защита от възможността да бъде откраднато хардуерното устройство (респективно чип картата и нейния четец заедно с пинкода за достъп) или умишлено да бъде предадена информация за достъп на трети лица.

Биометричното разпознаване се утвърждава все повече като сигурен механизъм за автентификация. Тя може да се осъществи чрез разпознаване на пръстов отпечатък или на лицето, сканиране на ириса или друга биометрична технология. Все по-широко приложение намират първите две техники [4, с. 10]. От изключителна важност е обаче да се осигури спазването на законосъобразната защита на биометричните данни. Същест-



Фигура 1. Пример за трифакторна автентификационна процедура [10]

вуващата, макар и минимална, потенциална възможност за кражби от базата данни с биометричните потребителски характеристики може да предизвика огромни проблеми. Компрометирането на подобна информация означава въвеждане на нова система за идентификация поради невъзможността за подмяна на биометричните потребителски характеристики.

Многофакторната автентификация в практиката. Примерът на Великобритания

Поради факта, че в САЩ са регистрирани най-много измами в резултат на кражби на самоличност, процесите по въвеждане на многофакторна автентификация на потребителите на уеб базирани финансови услуги там са в най-напреднал етап. Този етап отговаря на регулациите, установени от надзорната банкова институция в САЩ Federal Financial Institutions Examination Council (FFIEC)[8].

Според издаденото от съвета през 2005 г. „Ръководство за автентификация в условията на интернет банкиране" (Guidance on Authentication in an Internet Banking Environment) всички банки и други финансови институции, предлагащи уеб банкиране и други онлайн услуги, трябва да установят съответствие между нивото на автентификация и рисковете, свързани с предлаганите продукти и услуги. По тази причина от финансовите институции се изисква да организират риск мениджмънт за идентифициране на типа и нивата на риска, свързан с техните приложения за интернет банкиране. Там, където оценката на риска показва, че използването на еднофакторна автентификация е недостатъчно, финансовите институции трябва да прилагат многофакторна автентификация и да предложат сигурност на различни нива.

В съответствие с тези изисквания най-голямата банка в САЩ – Bank of America, е въвела многофакторна автентификация с използването на т.нар. „SiteKey security feature", който се базира на метода „Поделени тайни" и се състои от 3 части: уникално изображение, избрано от потребителя; уникална фраза, придружаваща изображението; и три въпроса, чийто отговор знае единствено потребителят. Съобразно оценката на риска, както се изисква според регулациите, са установени различни нива на сигурност – например при вход в системата за онлайн банкиране от обичайния IP адрес (компютър) клиентът трябва да разпознае изображението и надписа му и след това да въведе парола. В случай че влиза в приложението от неразпознат компютър, системата изисква от него въвеждане на потребителско име, отговор на един от трите въпроса, проверка за коректността на изображението и надписа му и едва след това въвеждане на парола. По този начин се реализира гъвкава многофакторна автентификация, при това клиентът може със задоволителна сигурност да използва интернет банкирането и от друг компютър, различен от обичайния.

Практиката на многофакторната автентификация в **Европа** е многообразна и се основава на използването на комбинация от различни методи. Сред утвърждаващите се тенденции е тази да се прилагат различни технически устройства за сигурност, от типа на посочените по-горе **токъни (tokens)**.

[8] FFIEC – съветът е създаден през март 1979 г., за да определя единни принципи, стандарти и форми за отчети и да създава единство в надзора на финансовите институции.

Един от вариантите за многофакторна автентификация предвижда да се използват банковите чип карти[9]. Предпоставка за това е напредналата в Европейския съюз фаза на миграция към чип базираната технология за дебитни и кредитни карти, която се основава на проекта EMV.

Името на проекта се формира от инициалите на консорциума от три компании Europay International, Mastercard International и Visa International[10], който разработва глобален стандарт за електронни финансови транзакции, основаващ се на чип карти. Новият стандарт се въвежда не само за използване на платежните карти на терминални устройства ATM и POS задължително заедно с пинкод (персонален идентификационен номер), но новата генерация смарт карти може да намери приложение за онлайн транзакции през компютър или мобилно устройство, в случай че потребителят разполага с четец. Благодарение на вградената в картите компютърна чип технология данните се криптират и по този начин се осигурява висока степен на защита. На практика е невъзможно копирането им върху друг носител, за разлика от досега използваните карти с магнитна лента.

EMV миграцията представлява за банките сложен и доста скъп проект, при това не съвсем доброволен. Той се стимулира активно с помощта на икономически санкции от двете картови организации – Visa и MasterCard. Изключително големите финансови инвестиции в EMV миграцията карат банките да се възползват и от някои допълнителни възможности на чип картите, осигурени чрез записване в паметта им на нови приложения. Сред тях е **използването им за сигурно разпознаване на потребителите при извършване на операции в системите за онлайн банкиране.** Това гарантира на банките постигане на по-голяма икономическа възвръщаемост от прилагането на чип картите в практиката.

Тази възможност предстои да бъде използвана от някои банки във Великобритания с цел да се осигури по-надеждна защита на потребителите на услуги през комуникационния канал интернет, при това важна предпоставка е приключилата миграция към банкови чип карти. Към края на януари 2006 г. 99 % от картодържателите във Великобритания (т.е. 41,5 млн. картодържатели) имат поне една чип карта [7]. От началото на миграцията през октомври 2003 г. са издадени общо 128 млн. чип карти, от които 65 млн. дебитни и 63 млн. кредитни карти. Това позволява банковите институции да ги използват активно като средство за многостранна автентификация на потребителите на онлайн банкирането.

До края на 2007 г. няколко от най-големите банки във Великобритания – **Barclays**, **NatWest** и **Nationwide,** реализират проекти за доставка на клиентите си (физически лица и представители на малкия и средния бизнес) на *четци на смарт карти* и *токъни, генериращи пароли*. Проектът на **Barclays** предвижда например банката да осигури безплатно на първо време за повече от 500 хиляди от потребителите на интернет банкирането четци на чип карти. Според пазарната си капитализация Barclays е третата по големина банка във Великобритания и деветата в ЕС. Предоставените от нея данни сочат, че към края на 2006 г. онлайн банкирането ѝ има над 1,7 млн. потребители и чрез него са извършени 214 млн. транзакции[11]. Проектът

[9] Понятията чип карта и смарт карта се използват като синоними.
[10] Понастоящем в консорциума участва третата голяма картова система JCB.
[11] http://www.newsroom.barclays.com/content/detail.asp?ReleaseID = 1013&NewsAreaID = 2

за използването на чип картите за автентификация, наречен „PINsentry", предстои да се реализира поетапно. Нивото на автентификация е разделено на различни нива съобразно оценката за равнището на риск. Така например клиенти, които извършват само справочни операции или извършват регулярни плащания (като например на комунални услуги), няма да се нуждаят от PINsentry. Системата ще се прилага задължително за физически лица и представителите на малкия и средния бизнес, които извършват плащания към сметки на трети лица *за първи път*, както и за новите клиенти. В този случай, освен обичайното въвеждане на потребителско име и парола, при логване в уеб сайта на банката потребителят трябва да постави своята EMV дебитна или кредитна карта в четеца и да въведе своя пинкод, след което токън устройството генерира случайно 8-цифрено число, което той трябва да въведе в сайта, преди да се авторизира транзакцията. За всяка транзакция се генерира ново число. По този начин, чрез няколко автентификационни признаци, се реализира сигурно потвърждаване на самоличността на клиента.

Подобни са проектите за многофакторна автентификация при онлайн банкирането и на другите две банки от групата на петте най-големи банки във Великобритания – **NatWest** и **Nationwide**[12]. При друга представителка на най-мощните кредитни институции – **Lloyds TSB**, проектът не предвижда използването на банкови чип карти, а е свързан с доставяне на потребителите на токън устройства с вграден чип и с генериране на случайни числа.

Осигуряването на високо ниво на защита дава възможност банките да предоставят на своите клиенти „Гаранция за онлайн банкирането" (напр. „Online Banking Guarantee" при Barclays[13] или „Internet Banking promise" при Nationwide) за възстановяване на евентуални загуби, причинени на клиента от измама чрез интернет. Така клиентите могат абсолютно спокойно да използват уеб базирания дистрибуционен канал, а банките от своя страна могат да разчитат на нарастване на броя на потребителите на иновативните им услуги, носещо им сериозни финансови ползи.

Практиката обаче показва, че успешните методи за автентификация при онлайн банковите услуги зависят не само от прилаганата технология, но в значителна степен от действията на потребителите и тяхната информираност, бдителност, самосъзнание и усещане за риск. Ето защо, освен да инвестират в проекти за сигурна автентификация на потребителите, които са приключени или в процес на реализация, банките във Великобритания работят изключително активно по обучението на своите потребители. В техните сайтове се отделя голямо внимание на опасностите, свързани с онлайн защитата, видовете зловреден софтуер и потенциалните начини за заразяване с него, необходимите мерки за предпазване от кражба на лични данни, препоръчват се конкретни антивирусни и други програми и пр.

С цел подпомагане обучението на потребителите и по-успешно противодействие на мрежово базираните банкови измами са разработени специализирани сайтове като **Banksafe Online** (http://www.banksafeonline.org.uk) и **Get Safe Online (**http://www.getsafeonline.org), които дават обширна информация за сигурно банкиране в реално

[12] Nationwide ("Nationwide Building Society") е строително дружество на кооперативен принцип, в което вложителите имат права, подобни на акционери в компания. Активите му към април 2007 г. са 137 млрд. лири и според този показател е сред първите банки във Великобритания.
[13] http://www.personal.barclays.co.uk/BRC1/jsp/brccontrol?site = pfs&task = homefreegroup&value = 13491

време и способи за самозащита. Сайтовете предлагат подробни разяснения за типовете измамнически софтуер и множество конкретни примери за измамни фишинг имейли. Освен това те събират обратна информация от потребителите за подозрителна електронна поща и фалшиви уеб сайтове.

Защитата срещу кражби на самоличност в българските банки

Случаи на кражби на самоличност се регистрират не само сред потребители на интернет банкирането на банките в чужбина, но и сред клиентите на българските банки. У нас обаче липсва статистика за броя на случаите и стойността на източените средства от банкови сметки. Единствено в печатните и електронните медии епизодично се съобщава за някои случаи, без опити за обобщения. По информация на отдел „Компютърни престъпления" към Главна дирекция „Борба с организираната престъпност" в България са регистрирани над 50 случая за източване на крупни суми от български банкови сметки само за половин година[14]. В съобщения от страна на прокуратурата също се споменава за случаи на кражби на самоличност, извършени от български граждани, като потърпевши са чужденци[15]. Като цяло се счита, че нивото на тези престъпления у нас е значително по-ниско, отколкото в развитите европейски страни.

Засега само една българска банка – Първа инвестиционна банка АД, съобщи в сайта си и чрез специални писма до потребителите на нейния виртуален банков клон за няколко случая на пробив в сигурността на системата за интернет банкиране. Настоятелната препоръка на банката е за закупуване на универсален електронен подпис от някой от четирите доставчици на удостоверителни услуги и по-специално от Инфонотари ЕАД, при което ползването на подписа през първата година е безплатно.

Повечето от опериращите на българския пазар банки и предлагащи интернет банкиране на своите клиенти, не отделят внимание на необходимостта от разясняване на проблемите и потенциалните опасности за сигурността на системите.

Ако разгледаме *групата на първите пет по големина банки* в зависимост от размера на активите им, установяваме, че три от тях игнорират потенциалния проблем и в сайта си не споменават за възможните неблагополучия, които грозят техните потребители, и за начините за реализиране на неавторизиран достъп – **Банка ДСК** (за ДСК Директ), **УниКредит Булбанк** (за системата Булбанк Онлайн) и **Обединена българска банка** (за U-online). Четвъртата по големина банка **Райфайзенбанк (България)** предоставя на клиентите си „Инструкция за сигурност", в която дава кратки и недостатъчно пълни съвети, свързани с ползването на „Райфайзен ОНЛАЙН". В тях на потребителите се обръща внимание да не отговарят на електронни съобщения, наподобяващи такива от банката и изискващи лични данни, и се акцентира на факта, че банката няма практика да обменя информация по електронна поща. По-изчерпателен е документът на **Първа инвестиционна банка** – „Основни препоръки с цел повишаване сигурността при работа с интернет банкирането на ПИБ АД", в който банката дава указания на потребителите си как да зареждат и различават истинността

[14] Информацията е цитирана от телевизия bTV на 17.10.2007 г. - http://btv.bg/news/?magic = bulgaria&story = 61245
[15] Източник: Прокуратура в Република България. Новини. http://www.prb.bg/php/newspage.php?news = %20 %20 %20 %20 %20873

на сайта ѝ, какви да бъдат препоръчителните настройки на браузера при работа със системата и др.

Съществуват и *положителни примери за банки* у нас, които се отнасят с необходимата отговорност към проблема за сигурността на системите за интернет банкиране, информираността на потребителите и запознаването им с възможните опасности. Съответстващи на практиката на западните банки са съветите на **ИНГ банк Н.В. – клон София,** в раздел „Сигурност" (публикувани във файл 2007_Security BG.doc). В интерес на потребителите съветите се отличават с голяма изчерпателност, актуализирани са през 2007 г. и съдържат подробни указания какво да направят клиентите, за да спомогнат за по-голямата сигурност на приложението за интернет банкиране. Добавянето на речник по защитата още повече увеличава достойнствата на политиката на сигурност на банката. Друг положителен пример са указанията, предоставени от **банка „Пиреос" – България** в раздел „Сигурност"[16] на Piraeus Online Banking. В тях се обяснява понятието „фишинг", посочва се необходимостта от използване на антивирусен и антишпионски софтуер и защитна стена на клиентския компютър, изисква се бдителност от потребителите и т.н.

Разглеждайки наличието на реализирани проекти за **сигурна многофакторна автентификация** в системите за онлайн банкиране **в банките в България**, можем да посочим, че засега такива се срещат сравнително рядко. Без да претендираме за изчерпателност, ще посочим някои банки у нас, които предлагат на клиентите си по-голяма сигурност на базата на повече автентификационни признаци. В **Сити банк Н.А. – клон София** – представителство на американската банка в България, всеки потребител на интернет банкирането (CitiDirect Online Banking) получава *персонално устройство за генериране на динамични пароли* (Safe Word карта). Благодарение на използването на еднократни пароли се елиминира опасността от евентуалното присъствие на шпионски софтуер на клиентския компютър и се осигурява сигурна автентификация с повече фактори.

ПроКредит банк (България), Българо-американската кредитна банка и **ЧПБ „Тексимбанк"** работят с уникални *еднократно използваеми шестцифрени кодове* – т.нар. TAN (транзакционен авторизационен номер), които се използват от потребителите за подписване на платежни нареждания към банката. Всеки потребител на интернет банкирането получава списък с TAN кодове и след изчерпването му банката го заменя с нов. Изпълнено е изискването за съответствие между нивата на риск и автентификация. Този способ за осигуряване на сигурна автентификация е сравнително стар, широко се използва в банките в Германия и е свързан с някои затруднения за клиента по повод необходимостта от получаването на новите списъци с TAN кодове на хартиен носител и опасността от загубването или откраднато им.

В банката със словенски акционерен капитал **НЛБ банка „Запад-Изток"** задължително се използват хардуерни устройства за авторизация – токън устройства (по-конкретно SafeNet Security iKey 2032). В техния чип се съхранява цифровият сертификат на потребителя, изискван за вход в системата за интернет банкиране. Устройството се включва към USB порта на клиентския компютър. Изпълняваните от клиентите платежни нареждания непременно се „подписват" с електронния подпис от устройството. По

[16] https://www.piraeusonline.bg/include/login/showWindow.asp?id = 78.lang = BG

този начин се осигурява двуфакторна автентификация на потребителите. Те обаче следва да платят според тарифата на банката еднократна такса за предоставяне на устройството, чийто размер не е за пренебрегване, особено за индивидуални клиенти[17], и следователно има ограничаващ ефект върху желанието им за ползване на услугата.

Същата технология се прилага и в **ИНГ банк Н.В. – клон София** от месец март 2007 г. За всички корпоративни клиенти при вход в системата за интернет банкиране ING Online се изисква цифров сертификат, инсталиран върху издадена от банката смарт карта. Целта е увеличаване нивото на сигурност чрез двуфакторна автентификация.

Според проучвания на автора още няколко банки подготвят проекти по въвеждане на многофакторна автентификация на базата на еднократно използваем транзакционен код. Сред тях е **Райфайзенбанк (България)**, която предстои да осигури на потребителите си персонални token устройства от тип Vasco[18]. Начинът за работа е с валидиране на заявка-отговор (request-response) в реално време – т.е. в сайта за интернет банкиране се генерира request – число с 6 или 8 цифри, които потребителят трябва да въведе чрез клавиатурата на персоналното си устройство. То от своя страна генерира response (пак 6 или 8 цифри), който потребителят въвежда обратно на сайта.

Обобщения и препоръки

Банките и другите институции, заинтересовани от борбата с кражбите на самоличност, трябва да **активизират** и **синхронизират** своите действия, първоначално на ниво Европейски съюз, а след това и на международно ниво, с оглед превенцията на подобни криминални действия на киберпрестъпниците. Към момента 6 от 10 европейски граждани смятат, че тези кражби са често срещани в техните страни, а около половината са на мнение, че националните мерки не са достатъчни и намират, че **решаването на този въпрос на ниво ЕС** ще бъде много по-ефективно, отколкото на национално ниво [2].

Някои стъпки в тази посока са направени, включително и с приемането през 2001 г. на Европейската конвенция за компютърните престъпления и подписването ѝ от 29 страни, между които САЩ, Япония и България.

Опасността от пробиви в системите за интернет банкиране и кражбите на самоличност в банките, работещи на българския пазар, не е за подценяване. Засега у нас преобладава информацията за случаи с действащи български киберпрестъпници основно извън границите на България, предимно поради по-големите наличности на средства по сметките на клиентите в западните банки. Това обаче не означава, че нашите банки могат да си позволят изоставане в превенцията на подобни неблагополучни събития.

Процесът за въвеждане на сигурна многофакторна автентификация на клиентите в съответствие с различните нива на риск в банките в международен мащаб е в напреднал стадий. Кредитните институции у нас следва за започнат работа, респективно да ускорят действията си по тези проблеми с оглед да преодолеят изоставането си.

Българските потребители все още не са наясно за големите опасности, с които могат

[17] Към момента таксата е EUR 70.
[18] http://www.vasco.com/products/product.html?product = 48

да се сблъскат при ползването на интернет банкирането. Следователно *по отношение на тяхното обучение банките у нас тепърва следва да поставят началото*. Засега повечето банки се задоволят само да предупреждават клиентите си предимно, че не комуникират с тях по електронна поща. В сайтовете им, с малки изключения, липсват разяснения, речници и примери, включително и с картинки, относно същността и начините за извършване на е-престъпления, свързани с кражбата на самоличност – фишинг, фарминг и пр. Добър пример в това отношение би могъл да бъде например сайтът на банка **Barclays** в раздел „Online Personal Banking", „Online security"[19].

В българското законодателство е необходимо да се въведе защита на потребителите на интернет банкиране от загуби, настъпили в резултат на неавторизиран трансфер или теглене на средства от сметка, така както е направено това например във Федералните банкови регулации в САЩ. В тях отговорността на потребителите се разглежда в 3 случая – до *$50, $500* или *цялата сума*, в зависимост от срока, в който потребителят научи и съобщи на своята банка за неавторизираните онлайн транзакции. В момента българските потребители сами носят отговорността и последиците за евентуални неблагополучия с техните средства, настъпили чрез системите за онлайн банкиране.

За разлика от банките в развитите страни, които по собствена инициатива поемат пълна гаранция за 100-процентно покриване на загубите на клиентите от неавторизирани транзакции, банките у нас декларират предварително в общите си условията за интернет банкиране или в договорите, че не носят вина за вреди, причинени от намесата на трети лица в системите. Такива текстове се откриват в условията за онлайн банкиране например на УниКредит Булбанк и Банка ДСК, като и двете са представителки на групата на най-големите банки в България. Подобни декларации не отговарят на стандартите за добра банкова практика и не са в интерес както на потребителите, така и на самите банки, тъй като, защитавайки своите клиенти, банките осигуряват защита на своя бизнес.

Необходимо е да се създаде институция, която има координиращи функции в сътрудничеството между търговските банки, БНБ, банковите клиенти и софтуерните разработчици на системи за електронни финансови услуги по повод на киберпрестъпленията, свързани с онлайн банкирането – събиране на статистика за случаите, предприемане на съвместни мерки за превенция, налагане на общи стандарти за сигурност, инициране на предложения за законодателни промени и пр. Организационната форма би могла да бъде асоциация, работна група или комитет. Според нас водеща роля в нея би следвало да изпълняват търговските банки, поради което, ако организационната форма е комитет, той би могъл да бъде създаден към Асоциацията на търговските банки.

В **заключение** може да се посочи, че инвестирането от страна на банките в проекти за реализиране на многофакторна автентификация на потребителите на онлайн банкови услуги е надеждно средство за предотвратяване на кражбите на самоличност и осигурява изискваната висока степен на тяхната защита. Това от своя страна гарантира запазване на възходящата тенденция в изменението на броя на потребителите на уеб базираното банкиране.

[19] http://www.personal.barclays.co.uk/BRC1/jsp/brccontrol?task = channelFWgroup&value = 8722&target = _ blank&site = pfs

Литература

1. Арсенов, А., Биометрията се завръща в бизнеса, CIO, 2005, № 4, с. 48-52.

2. Прессъобщение по повод конференция на тема: „Поддържане на интегритета на идентичността и плащанията: две предизвикателства за превенция на измамите", Брюксел, 22.11.2006 г. http://www.evropa.bg/bg/del/info-pad/news.html?newsid = 2337

3. Andersen, N., The Threat of Cybercrime: The Challenge of Online Identity Theft and Strengthening the Public-Private Partnership in a Changing Threat Environment, доклад, изнесен на конференция на тема „Поддържане на интегритета на идентичността и плащанията: две предизвикателства за превенция на измамите", Брюксел, 22.11.2006 г.

4. Federal Financial Institutions Examination Council: Guidance on Authentication in an Internet Banking Environment – October 2005.

5. http://www.barclays.co.uk

6. http://www.banksafeonline.org.uk

7. http://www.chipandpin.co.uk

8. http://www.id-protect.co.uk/index.php

9. http://www.michigan.gov/cybersecurity/0,1607,7-217-34415---,00.html

10. http://www.unidentity.com

11. http://www.vasco.com ИА