УДК 002.513

Л. М. Ткачук
І. В. Леонтьєв

МЕТОДИ ЗАХИСТУ УКРАЇНСЬКИХ БАНКІВ ВІД КІБЕРАТАК

Вінницький національний технічний університет

Анотація
Запропоновано методи запобігання виконання кібератак у банківській сфері України, що дозволить відновити довіру вкладників, користувачів, інвесторів до банків, особливо державних, та використовувати їхні можливості в повному обсязі.
Ключові слова: NFS, вірус-троян, IT-департамент, CISO (Chief Information Security Officer), DLP (Data Loss Prevention).

Abstract
Methods of preventing cyber attacks in the banking sector of Ukraine have been proposed, which would allow to fully restore the confidence of depositors, users, investors in banks, especially state-owned ones, and to make full use of their services.
Keywords*:* NFS, Trojan virus, IT department, CISO (Chief Information Security Officer), *DLP (Data Loss Prevention).*

Вступ

Останнім часом функціонування інформаційних систем у світі виявило проблему недостатньої захищеності від комп'ютерних вірусів. BadRabbit, WannaCry, Petya та інші вражали несподівано, паралізуючи комп'ютерні системи різних установ та підприємств. Їх розробники хоча й мали подекуди різну мету та способи впровадження вірусних програм, однак базувалися на спільному підґрунті – недоліках і слабкостях системи кібербезпеки.

Доволі ілюстративним у цьому питанні видається механізм дії вірусу Petya, який за кілька днів завдав мільйонних збитків українському бізнесу та державним установам. Вірус непомітно вражав популярну програму бухгалтерського забезпечення M.E.Doc., отримував доступ до адміністративних прав керування комп'ютерною системою та безперешкодно поширював власні копії. Не стали винятком банківські установи, які повинні бути захищеними сучасним технічним та системним забезпеченням. Світовий досвід атак вірусів і значних фінансових втрат мав стимулювати, насамперед, саме фінансові установи до пошуку прогалин власних систем кіберзахисту та їх постійного оновлення. Однак 2017 р. показав фактичну неготовність українських банків захисти себе від подібних втручань у роботу їхніх інформаційних систем. Загальна оцінка подій 27-29.06.2017 р. демонструє, що 70% українських банків певним чином постраждали від кібератак вірусу Petya. Видимим наслідком таких атак стала зупинка роботи терміналів, платіжних систем, відділень банків, а також обмежений доступ до інтернет-банкінгу та міжнародних переказів.

Хоча банки продовжують стверджувати, що атаки негативно вплинули винятково на інфраструктуру системи Windows, а вірус не отримав доступу до персональних баз даних клієнтів, не можна бути впевненим, що більш «витончена» програма не зможе цього зробити. Той факт, що банки не витримали кібератак, спонукає до висновку, що проблема полягає не лише в IT департаменті кожного окремого банку. Недооцінка потенційних загроз, відсутність належного програмного забезпечення та нехтування належним бюджетуванням систем кібербезпеки банку – все це свідчить про недостатність системного підходу до забезпечення кібербезпеки [1].

Результати дослідження

Високій рівень інформаційної безпеки забезпечується захистом всіх ланок системи Інтернет-Банкінгу – від захисту серверів та веб-сайту банку до авторизації та шифрування платіжних документів у клієнта.

Для цього використовуються такі механізми:

– *Автентифікація серверу Інтернет-Банкінгу*: для забезпечення захисту від атак на банківський веб-сервер, підміни або модифікації його контенту використовується SSL-протокол з'єднання та сертифікат відкритого ключа стандарту X.509 від міжнародного засвідчувального центру Thawte.

– *Автентифікація клієнтів Інтернет-Банкінгу*: застосовується технологія багатофакторної автентифікації користувачів на базі таємних криптографічних ключів, що зберігаються на спеціальних апаратних носіях ключової інформації (НКІ типу USB-Token), в якості додаткового фактору можливе використання одноразових паролів (OTP-паролів).

– *Шифрування даних*: за допомогою захищеного мережевого SSL-протоколу забезпечується конфіденційність даних, якими обмінюються клієнти з сервером Інтернет-Банкінгу у мережі Інтернет, виключається можливість перехоплення та несанкціонованого читання платіжної та іншої інформації.

– *Авторизація платіжних документів*: механізм електронного цифрового підпису забезпечує автентичність та цілісність електронних платіжних документів. Для перевірки або формування електронного цифрового підпису до системи Інтернет-Банкінгу інтегровані засоби криптографічного захисту, що сертифіковані відповідно до вимог чинного законодавства України.

Для підвищення рівня інформаційної безпеки додатково можуть використовуватись IP-фільтрація (індивідуальні для кожного клієнта обмеження переліку IP-адрес, з яких дозволено з'єднання с сервером Банку), SMS-оповіщення (інформаційні повідомлення про події в системі Інтернет-Банкінгу від імені Клієнта), OTP-пароль підтвердження окремого платежу.

Обов'язковою умовою підключення до системи Інтернет-банкінгу є використання з боку Клієнта підвищеного рівня захисту системи на базі апаратного НКІ [2].

Одна з систем, що забезпечує захист інформації - це DLP (Data Loss Prevention) – система та інші засоби, що захищають від витоків, перекривають або контролюють канали, за якими інформація може залишити інформаційну систему, такі як мережеві з'єднання по різних протоколах, відчужувані носії інформації, мобільні комп'ютери, принтери тощо.

Не завжди у банків вистачає коштів і умінь перекрити всі можливі канали. Ті носії, які залишаються без належного контролю, є провідниками відповідної частки випадкових витоків. У відношенні умисних витоків ситуація значно гірша. Внутрішні зловмисники, знаючи, які саме канали контролюються, намагаються їх обійти і послати конфіденційні дані по вільному, незахищеному каналу. Тому на ймовірність умисних витоків слабко впливає неповне перекриття параметра інформаційної системи. Щоб ефективно протидіяти як випадковим, так і умисним витокам, DLP система (за підтримки організаційних заходів), зрозуміло, повинна охоплювати всі без винятку канали (носії). Результати аналізу основних каналів витоку інформації у світі, здійсненого компанією Infowatch, узагальнено в таблиці 1 [3].

Таблиця 1 – Можливості витоку інформації у банках

Канали витоку	2016		2017	
	Кількість	Відсотки	Кількість	Відсотки
Мобільний комп'ютер	49	11,9	40	10,5
Носії інформації (CD/DVD, флешносії)	23	5,6	32	8,4
Настільний комп'ютер, сервер, НЖМД	41	9,9	90	23,6
Інтернет (вкл. e-mail)	97	23,5	82	21,4
Паперовий документ	84	20,3	78	20,4
Архівний носій	48	11,6	6	1,6
Інший	36	8,7	25	6,5
Не електронні	35	8,5	29	7,6

За оцінками аналітиків Infowatch, впровадження шифрування мобільних носіїв буде продовжуватися, але дуже повільно. Все, що можна було запровадити «добровільно», вже зроблено. Подальше поширення шифрування можливо лише за рахунок адміністративного ресурсу – спочатку на корпоративному та галузевому рівнях, потім, можливо, на державному. Однак число використовуваних мобільних носіїв (ноутбуків і флеш-накопичувачів) постійно зростає. За рахунок цього частка «мобільних» витоків може знову вирости.

Паперовий документообіг проконтролювати складніше, ніж електронний. Після виходу листа з принтера стежити за ним можна лише «вручну», за допомогою людей і організаційних процедур. В умовах відносної дешевизни технічних рішень і відносній дорожнечі робочої сили не дивно, що на Заході контроль за паперовими носіями слабкіше контролю за комп'ютерною інформацією.

До того ж, недосконалі засоби захисту від витоків (назвати їх повноцінними DLP- системами ми не можемо) не контролюють такий канал, як відправка на друк. У цьому випадку конфіденційна інформація легко виходить з-під контролю. Типовий «паперовий» витік - це збій при автоматичній роздруківці листів, адресованих великому числу клієнтів. Як відомо, адреса на листі або на конверті друкується теж автоматично, часто і конверти заклеює автомат. Невелике зміщення - і адресати в листі і на конверті (в адресі) перестають збігатися, листи з чужими персональними даними йдуть стороннім людям. Щоб знизити число «паперових» витоків, необхідні два заходи. По-перше, потрібна DLP-система, яка блокує відправку на друк недозволеної інформації та перевіряє відповідність поштової адреси і адресата [4].

По-друге, необхідний комплекс організаційних заходів щодо обліку руху паперових документів з конфіденційною інформацією. Заходи ці досить дорогі (особливо натлі низької вартості принтерів), тому число інцидентів з паперовими носіями буде знижуватися дуже повільно - в основному за рахунок відмови від використання паперу взагалі.[4]

Висновки

Отже, основні проблеми захисту банків від загроз зумовлені їх недостатньою увагою до власної безпеки економічної інформації. Реалізація зазначених заходів дозволить мінімізувати ризики витоку конфіденційних даних. Не втратити довіру клієнтів і не перетворитися на черговий об’єкт статистики інцидентів у сфері інформаційної безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України «Про банки і банківську діяльність» від 17.01.2001 // Відомості Верховної Ради України. - 2001. - № 4.

2. Закон України «Про інформацію» // Ст. 30 «Інформація з обмеженим доступом».

3. Зубок М. І. Безпека банківської діяльності: навч. посіб. / М. І. Зубок. - К.: КНЕУ, 2009. - 190 с.

4. Аналітичні дані інформаційної безпеки - www.infowatch.ru

Ткачук Людмила Миколаївна – доцент кафедри менеджменту та безпеки інформаційних систем, кандидат економічних наук, заступник декана з навчально-методичної роботи Факультету менеджменту та інформаційної безпеки ВНТУ, e-mail: ludatkachuk2017@gmail.com.

Леонтьєв Ігор Віталійович – студент групи КІТС-18б факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: leontiev3igor@gmail.com.

Tkachuk Lyudmyla Mykolayivna – associate professor of Department of Management and Security of Information Systems, candidate in economics, deputy dean for educational and methodological work of the Faculty of Management and Information Security of VNTU, e-mail: ludatkachuk2017@gmail.com.

Leontiev Igor Vitaliyovych - student of KITS-18b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: leontiev3igor@gmail.com.