УДК 004.056

Р. М. Алгулиев, Я. Н. Имамвердиев, Ф. Д. Абдуллаева
Институт информационных технологий,
Национальная академия наук Азербайджана, Азербайджан, Баку

ВЕКТОР АТАКИ И ЗАЩИТНЫЕ МЕРЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рассматривается проблема обеспечения безопасности персональных данных. Излагается понятие вектора атаки персональных данных технического, физического и социально-инженерного характера. Понятие «кража данных» описывается как реальная угроза широкого использования персональных данных. На основе методики управления рисками предлагается подход к снижению рисков краж персональных данных.

В настоящее время, несмотря на ускоренное развитие отрасли информационной безопасности в целом, количество инцидентов безопасности продолжает увеличиваться. Причиной увеличения инцидентов безопасности является наличие недостатков в разработанных программных продуктах, нацеленных на решение задач информационной безопасности.

Экспансия информационных технологий в производство и управление современных организаций предопределяют рост информационных инфраструктур организаций, что зачастую приводит к неструктурированному гетерогенному характеру компьютерных сетей и является основой неконтролируемого роста уязвимостей, а также к увеличению возможностей несанкционированного доступа к информации.

Несанкционированный доступ к записям, содержащим персональные данные индивидуума, приводит к возникновению брешей данных.

Брешь данных (data breach) – это неавторизованное приобретение электронных данных, компрометирующее безопасность, конфиденциальность, целостность персональной информации [1]. Это понятие также известно, как брешь в системе защиты (*security breach*) или как брешь секретности (*privacy breach*).

На основе данных центра ITRC (*Identity Theft Resource Center*, ITRC), уведомления субъектов о наличии брешей были помещены в одну из следующих категорий [2]:

– учебные заведения: все уровни государственных и частных учебных предприятий, включая колледжи, университеты, аффилированные объекты (например, организации выпускников);

– организации здравоохранения: больницы, службы здравоохранения, страховые компании;

– организации по управлению финансами: банки, страховые компании и инвестиционные услуги;

– предприятия общего назначения: коммерческие организации, не имеющие отношения к вышеперечисленным категориям;

– правительственные организации: федеральные, государственные и муниципальные организации.

Бреши в системе защиты классифицируются по причинам их возникновения [2]:

– хакер: нелегальный доступ через Интернет человека, находящегося вне атакованном объекте, к данным, содержащимся в компьютерной системе;

– физическая кража: кража компьютеров, компьютерных оборудований (включая носители компьютерных данных) или бумажных файлов;

– чужой дисплей: позволяет просмотр персональной информации человеку, который не имеет к нему доступа;

– доступ изнутри: кража служащих и контракторов, предоставление предпринимателем доступа к персональной информации;

– потеря резервных оборудований: кража носителей, содержащих персональные данные;

– причины, не установленные: специфичная причина брешей, которая не была раскрыта субъектом, испытывающим потери данных.

Бреши безопасности, вытекающие от хакеров и внешних доступов, имеют наибольший разрушительный потенциал. Эти бреши завершаются преднамеренными попытками для получения доступа к персональной информации. При наличии перечисленных типов брешей персональная информация приобретается субъектом или передается субъекту, стремящемуся совершать кражу данных (*Identity Theft*).

Борьба с кражами данных является актуальной и жизненно важной проблемой. С целью составления статистических данных о краже персональных данных в зарубежных странах созданы специальные центры:

– *Identity Theft Data Clearinghouse* (http://www.ftc.gov);

– *Privacy Rights Clearinghouse* (http://www.privacyrights.org);

– *Identity Theft Resource Center* (ITRC) (http://www.idtheftcenter.org).

По данным центра *Privacy Rights Clearinghouse*, 85 % организаций сталкивались с проблемой кражи персональных данных. За период 2005–2009 гг. было украдено 260 716 323 записи СУБД.

Многие толкователи отмечают, что термин «кража данных» (*identity theft*) в общем, используется для выражения термина «подделка данных» (*identity fraud*), в котором «кража» (*theft*) и «подделка» (*fraud*) должны разъединяться [3]:

– подделка (*fraud*): обман, который умышленно осуществляется, чтобы обеспечивать несправедливую и незаконную выгоду;

– кража данных (*identity theft*): получение персональной или финансовой информации, присущей другому человеку, с целью создания ложной идентификации. Кража данных соответственно охватывает множество действий, включая сбор персональной информации, создание ложных документов личности и использование персональной информации обманным путем.

В табл. 1 указаны персональные данные человека, которые злоумышленники часто стараются приобрести.

Таблица 1

Персональные данные человека

Название	Гендер	Возраст
Дата рождения	Место рождения	Свидетельство о рождении
Девичья фамилия матери	Семейное положение	Этническое происхождение
Адрес (текущий и прежний)	Телефонный номер	Адрес электронной почты
Номер социального страхования	Лицензионный номер водителя	Номер медицинской карточки
Номер паспорта	Карточка постоянного места жительства	Мандат счета (имя пользователя, пароль, ПИН и т. д.)
Трудовая книжка	Информация о семье	История об образовании
История болезни	Число иждивенцев	Информация о супруге
Личный адрес	Номер диска транспортного средства	
Регистрационный номер транспортного средства	Информация о средствах	
Номера кредитной карточки	Номер визитной карточки и персональный идентификационный номер (ПИН)	Долги
Номера платежной карточки и персональный идентификационный номер (ПИН)	Идентификационный номер налогоплательщика	Фактические или ожидаемые доходы
Номера банковского счета	Подробности об ипотеке	Информация об инвестиции
Неуплаченный долг		
Отпечатки пальца	Отпечатки голоса	Изображение сетчатки
Высота	Вес	Цвет глаз и волос

Злоумышленники для приобретения персональных данных пользуются многими методами. Эти методы называются *векторами атаки*, термин означает маршрут или способ, который используется для вторжения в компьютерные системы [4; 5].

Имеются три различных вида векторов атак:

1. *Технические* – атаки эксплуатируют компьютеры и подключения Интернет:

– *Trojan/Keystroke Logger* – программы-шпионы/вредоносные программы, помещенные посредством хакерства;

– *Wireless Intercept* – вооруженное нападение (*Wardriving*), открывает точку доступа, установка фальшивой точки доступа (*airsnarfing*). Атака *«Evil Twin»*;

– *Pharming – DNS* спуфинг, отравление кеша *DNS*, прокси атаки;

– *Scrape Web site* – сбор персональных данных из Веб-сайтов; поисковые системы Веб используются как верификатор;

– *Sniffing* – сбор пакетов данных атакуемой сети;

– *Hacking* – получение привилегированного доступа к компьютеру для осуществления дальнейших нападений и/или сбор данных;

– *Data attacks – SQL Injection, XSS*;

– *Database attacks – Login attacks, inference attacks, SQL* сканеры;

– *Password cracking* – приобретение паролей администратора к серверам.

2. *Физические* – атаки, связанные с такими устаревшими технологиями, как отслеживание мусора:

– *Theft* – кража портативных компьютеров, бумажников, почты;

– *Shoulder Surfing* – непосредственное наблюдение персональной информации;

– *Dumpster Diving* – приобретение отброшенных документов, аппаратных средств (дисков);

– *Trusted Insiders* – персональная информация, неправильно использованная индивидуумами при доступе;

– *Breach firewall(s)* – присоединение к внутренней сети.

3. *Социально-инженерные* – атака, использующая особенности человека в своих интересах, чтобы получить персональную информацию:

– *Phishing* – соблазнение индивидуумов, чтобы показать конфиденциальные данные;

– *Family members* – персональные данные, ошибочно использованные членами семьи;

– *Legal Sources of Identity* – получение персональных данных от кредитных бюро, правительственных агентств мошенническим путем;

– 419 *scams* – получение денег или информации о счете;

– *Trusted Insiders* – получение персональной информации от провайдеров (докторов, стоматологов, юристов, администраторов баз данных, служащих, контракторов, индивидуумов и т. д.);

– *Gain access* – получение доступа в компьютерные залы, коммутационные шкафы, коммутаторы, маршрутизаторы;

– *Phone requests* – получение персональной информации, чтобы облегчать хакерство.

Отметим, что перечисленные атаки ставят персональные данные под угрозу подвергания риску их краж. Имеется ряд защитных мер, которые могут быть предприняты для минимизации рисков, вытекающих от вышеперечисленных атак. Выбор защитных мер должен осуществляться на основе их эффективности. При этом определение критерия выбора конкретных защитных мер является более сложной задачей. Подходы оценки и управления рисками являются эффективными механизмами в этом процессе отбора.

Оценка рисков подразделяется на три основные этапа: определение серьезности последствия угрозы, определение вероятности возникновения угрозы и проведение на основе этих двух факторов оценки рисков [6]:

Риск = Вероятность возникновения × Серьезность последствия.

Если предположить, что эти два фактора точно определены, то метод оценки рисков окажет помощь при выборе защитных мер, препятствующих конкретной атаке. Соответствующие защитные меры, избранные с применением метода оценки рисков в контексте персональных данных, иллюстрированы в табл. 2.

Таблица 2

Защитные меры персональных данных

Защитные меры / Инциденты	Многофакторная аутентификация	Антивирусная защита	Шифрование	SSL/TLS	Контроль доступа	Обучение пользователя	Соблюдение политики безопасности	Аудитный контроль
Trojan/ Keystroke Logger	√	√						
Wireless Intercept			√					
Pharming				√				
Scrape Web site								
Sniffing				√				
Hacking					√			
Data attacks								
Database attacks	√		√					
Password cracking	√							
Theft			√			√	√	
Shoulder Surfing						√		
Dumpster Diving						√		
Trusted Insiders	√		√		√	√		√
Breach firewall(s)								
Phishing	√							
Family members						√		
Legal Sources of Identity	√							
419 scams						√		
Gain access	√					√		
Phone requests						√		

Библиографический список

1. Romanosky, S. Do Data Breach Disclosure Laws Reduce Identity Theft? / S. Romanosky, R. Telang, A. Acquisti. Seventh Workshop on the Economics of Information Security. Hanover, 2008.
2. ITRC Breach Meter Reaches 342, to Date 2008 Data Breach count is 69 % greater than 2007 (Jan 1 through June 27) [Электронный ресурс]. Режим доступа: http://www.idtheftcenter.org/artman2/publish/m_press/Breach_List_2008_Q2.shtml. Загл. с экрана.
3. Identity theft and protecting personal information // Plymouth Chamber of Commerce. Brown Bag Lunch Series. 2009.
4. Techniques of Identity Theft: CIPPIC Working Paper. ID Theft Series / Canadian Internet Policy and Public Interest Clinic. 2007. № 2.
5. Liberty Alliance Whitepaper: Identity Theft Primer [Электронный ресурс] // Liberty Alliance Project. Режим доступа: http://www.projectliberty.org/resources/id_Theft_Primer_Final. Загл. с экрана.
6. General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, GAO // AIMD, 1999.

R. M. Alguliev, Ya. N. Imamverdiev, F. D. Abdullaeva

Institute of Infortion Technology, Azerbaijan National Academy of Sciences, Azerbaijan, Baku

ATTACK VECTORS AND DEFENSIVE MEASURES OF PERSONAL DATA

In this paper the problem of security of the personal data is considered. Concept of attack vectors of the personal data in technical, physical and social - engineering character is described. The «Identity Theft» concept is described as a real threat of the wide implementation of personal data. On the basis of risk management technique is offered the approach reducing risks of personal data thefts.

E-mail: secretary@iit.ab.az, yadigar@lan.ab.az, farqana@iit.ab.az

УДК 004.8.032.26

О. О. Варламов

ООО «МИВАР», Россия, Москва

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И АНАЛИЗ ДЕВЯТИ ВИДОВ ТЕХНИЧЕСКОЙ КОМПЬЮТЕРНОЙ РАЗВЕДКИ

Рассмотрены девять видов технической компьютерной разведки и особенности защиты персональных данных от них.

Выделяют агентурную и техническую разведки. В отличие от агентурной, техническая разведка непосредственно с людьми не работает. Образно говоря, при создании, передаче, хранении или обработке информации всегда можно выделить некий «материальный носитель» информации и ее «содержание» (смысл, семантика), между которыми всегда есть четкое взаимоотношение. Тогда информация – это «двойка», т. е. вектор,