УДК 004.056

Ю.А. Звягинцева, Ю.Н.Павлова

СОЗДАНИЕ ЭФФЕКТИВНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Данная статья посвящена вопросам создания эффективных систем защиты информации на предприятии. В рамках статьи рассматриваются основные виды угроз, которые возникают в процессе использования сети Интернет. Дается понятие IT-безопасности как в широком, так и в узком смысле этого слова. С учетом данных определений, проводится анализ основных угроз безопасности за 2011 год, рассмотрены наиболее часто встречающиеся виды угроз, которые могут нанести непоправимый вред как деловой репутации, так и основным показателям финансовой деятельности фирмы. На основе проведенного анализа предложены механизмы защиты информации предприятий всех форм собственности.

Ключевые слова: информационная безопасность, хактивисты, виртуальные карманники, мобильные угрозы, смарт-карты; биометрические системы; системы обнаружения вторжения ;межсетевой экран.

UDC 004.056

Ju.A. Zvyagintseva, Ju.N. Pavlova

CREATION OF EFFECTIVE INFORMATION SAFETY SYSTEM

The article is devoted to the questions of creation of effective information protection systems at the enterprise. The principal kinds of threats which arise while using the Internet are considered. The concept of IT-safety both in the wide, and in the narrow sense of this word is given. Taking into account the given definitions, the analysis of the basic safety for 2011 is carried out. The most often appeared kinds of threats which can cause irreparable harm both to business reputation, and the basic indicators of financial activity of a firm are considered. On the basis of the analysis information protection mechanisms of the enterprises of all forms of ownership are suggested.

Keywords: information safety, activists, virtual pickpockets, mobile threats, smart cards; biometric systems; detection systems of intrusion; firewall.

Сегодня информационные технологии - это не просто одна из вспомогательных функций предприятия, все чаще компьютерные системы являются главной основой всей деятельности организации. Но и одновременно с этим растет угроза нормальной, бесперебойной работы информационной системы. Наиболее яркий пример - это глобальная сеть Интернет, которая дает одновременно принципиально новый уровень эффективности использования IT для решения всевозможных бизнес-задач, но и наряду с этим является основным источником вредоносных программ, угрожающим стабильному функционированию деятельности компании. Самым заметным последствием таких программ является снижение производительности, выраженное невысокой отдачей на запросы вследствие всплывающих рекламных окон. Из-за этого меняются настройки, добавляются таинственным образом новые функции, в диспетчере задач отображаются новые процессы, выходят из под контроля программы. Однако многие пользователи продолжают вести себя легкомысленно, тем самым открывая вредоносным программам дверь настежь к своему компьютеру.

Сегодня никого не нужно убеждать в значительности проблемы IT-безопасности, она не только хорошо известна IT - специалистам, но и современным пользователям. К примеру, в Европе было проведено исследование, которое показало что более 80% руководителей склоны считать, что IT- безопасность имеет огромное значение для успешной работы организации, а более четверти из них утверждали, что отдача на инвестиции в сферу безопасности оказалась более высокой, чем ранее предполагалось [9]. Прежде чем рассматривать влияние угроз на информационную безопасность систем и процессов в обществе, необходимо уточнить понятие IT-безопасности, которое на сегодня понимается как в широком, так и в узком смысле.

IT-безопасность в широком смысле (Information security) - это свойство процесса информатизации и всей жизнедеятельности общества, которое гарантирует устранение всех негативных последствий информатизации, либо сводит их до такого минимума, который обеспечивает выживание и дальнейшее развитие человечества, его превращение в развитую, гуманную информационную цивилизацию [1].

В то же время под IT-безопасностью в узком смысле понимают совокупность свойств информации, связанных с обеспечением запрещения неавторизованного доступа (получения, ознакомления с содержанием, передачи, хранения и обработки), модификации или уничтожения, а также любых других несанкционированных действий с личной, конфиденциальной или секретной информацией, представленной в любом физическом виде [1]. Таким образом, информационная безопасность в современном обществе включает в себя:

- компьютерную безопасность;
- создание социальной среды необходимой для гуманистической ориентации информационных процессов;
- безопасность информационных систем и процессов в обществе.

Информационная безопасность не сводится только к компьютерной безопасности, так же как информатизация не тождественна компьютеризации общества. Поэтому понятие информационной безопасности, включая в себя компьютерную безопасность в качестве неотъемлемой составной части, должно распространяться на все информационные процессы в обществе и другие социальные процессы, в той или иной степени влияющие на информацию и средства информатики.

Проведя анализ статистики за указанный период 2011 год, мы к пришли к следующему выводу - он оказался еще более насыщен взломами, атаками, утечкой информации. Пострадали такие компании, как Citibank, Honda, Fox News, Epsilon, Sony, были украдены в большинстве случаев данные клиентов компании, при этом нет никакой информации о продаже этих данных на черном рынке или использовании злоумышленниками, следовательно, для хакеров конечная цель была не продажа краденой информации. В компании Sony произошла одна из самых крупных утечек в результате взлома сервера. По подсчетам данной компании, у злоумышленников могли оказаться данные 77 миллионов пользователей, однако на сегодняшний день нет в открытом доступе информации о том, кто и зачем провел данную атаку. Существует лишь предположение, что главной целью хакеров было пошатнуть репутацию мировой компании.

На сегодняшний день можно выделить следующие виды угроз, которые могут нанести непоправимый вред как деловой репутации, так и основным показателям финансовой деятельности фирмы:

1. Хактивисты.

«Хактивизм»-это волна взлома или вывода из строя различных систем в знак протеста против государственных органов или больших корпораций. Была создана новая группировка LulzSec, которая за 50 дней своего существования сумела взломать множество систем и опубликовать личную информацию десятков тысяч пользователей. Под удар данной группировки попали государственные органы: сенат США, SOCA UK,ЦРУ, крупные корпорации EA, Sony,AOL и т.д. Краденая информация публиковалась на их сайтах, затем размещалась в torrent-сети. Вскоре LulzSec объединилась с усилиями группировки Anonimous и получила политическую окраску. В результате атак хакеры получили доступ, в том числе к данным полиции Аризоны. В открытом доступе была размещена переписка сотрудников, персональные данные о сотрудниках, секретные документы и пароли некоторых сотрудников. Данное преступление, как заявили сами участники группировки, было направлено в знак протеста против решения сената Аризоны об ужесточении миграционной политики.

2. Виртуальные карманники.

Одной из угроз являются виртуальные карманники. Зашифрованный кошелек находится у пользователя на компьютере, но для того чтобы получить доступ, необходим пароль. С целью получения доступа пароля к кошельку злоумышленники разработали простую троянскую программу, работающее по следующему принципу: при запуске компьютера пользователя он отсылал по почте файл его bitcoin-кошелька хозяину вредоносной программы, что позволило списывать денежные средства с кошельков пользователей.

3. Trojan.NSIS.Miner.a (троянская программа, троянец, троянский конь)

Троян - это вредоносная программа, проникающая в компьютер под видом безвредной - кодека, скринсейвера, хакерского программного обеспечения и т.д. При написании простейшего троя используются языки программирования, такие как Visual Basic или C++. В середине 2011 года была обнаружена троянская программа, состоящая из легальной программы по созданию момент (bcm) и управляющего троянского модуля. После заражения компьютера вредоносная программа начинает генерировать монеты для злоумышленников. Зона охвата трояна – Вьетнам (3%), Индия(12%), Украина (7%), Казахстан (5%), Россия (37%). Но, к счастью, троянская программа была достаточно быстро обнаружена автоматической системой биткойн-пула, аккаунт хакеров был заблокирован, а затем успешно удален. Вскоре была обнаружена новая модификация опасной троянской программы-вымогателя GpCode, которая шифрует данные на зараженном компьютере и требует выкуп за расшифровку. Жертвами данного троянца стали жители Европы и постсоветской территории. Зона охвата вредоносной программы - Германия, Франция, Нидерланды, Казахстан, Россия, Украина. При этом злоумышленники требовали выкуп за расшифровку троянской программы на основе перевода денежных средств через систему электронных денег Ukash. Непродолжительный период распространения обозначает, что создатель трояна GpCode не старался к массовому заражению компьютеров из-за боязни разоблачения правоохранительными органами.

4. Мобильные угрозы.

Основной угрозой для мобильных устройств является вредоносное ПО. Проведенное лабораторией G Data SecurityLabs исследование показало, что в 2011 году доля вредоносных программ для смартфонов и планшетов увеличилась на 140% в соотнесении с общим количеством вредоносного ПО Эксперты отметили особую активность со стороны кросс-платформенных троянских программ, которые в данный момент превосходят на фоне других угроз. Большая часть из них была создана для распространения спама и прочей нелегальной деятельности, которую ведут электронные мошенники. Также существует серьезная опасность получения мобильного вируса через онлайн-магазины приложений App Store: вредоносное ПО распространяется только непосредственно с закачиваемыми приложениями. Связи с тем что подавляющее большинство владельцев смартфонов сегодня не используют мобильный антивирус для сканирования на наличие зараженных программ, это приводит к серьезной опасности. Кроме того, все чаще начинает встречаться угроза атаки через существующие беспроводные сети: мобильные устройства всё более восприимчивы к таким атакам, – существуют мобильные приложения, используя которые, злоумышленник легко получает доступ к электронной почте и социальным сетям «жертвы». Основными последствиями этой угрозы является перехват данных через GPRS,

3G или WI-FI сети. На телефон может поступить сообщение с настройками сети, сохранив и активировав которое, пользователь сменит точки доступа, куда и пойдет нужный мошенникам трафик. В настоящее время очень распространена схема монетизации большинства мобильных троянских программ, она связана с отправкой SMS-сообщений на короткие номера. В результате происходит списание денежных средств со счета пользователя, либо владельца телефона без его согласия подписывают на платный сервис.

Так, в 2011 году было зафиксировано 1 108 787 447 атак, проводившихся с Интернет-ресурсов, размещенных в разных странах мира. Всего в данных инцидентах было отображено 412 494 разных вредоносных и потенциально нежелательных программ. Если рассматривать территориальный аспект распространения вредоносных угроз, то наибольшее число хакерских атак зарегистрировано в Омане (55,7%), в России (49,5%) (рис.1). Таким образом, в 2011 году в десяти странах мира было сконцентрировано 87% веб-ресурсов, применяемых для распространения вредоносных программ (на 2% меньше, чем в прошлом году).

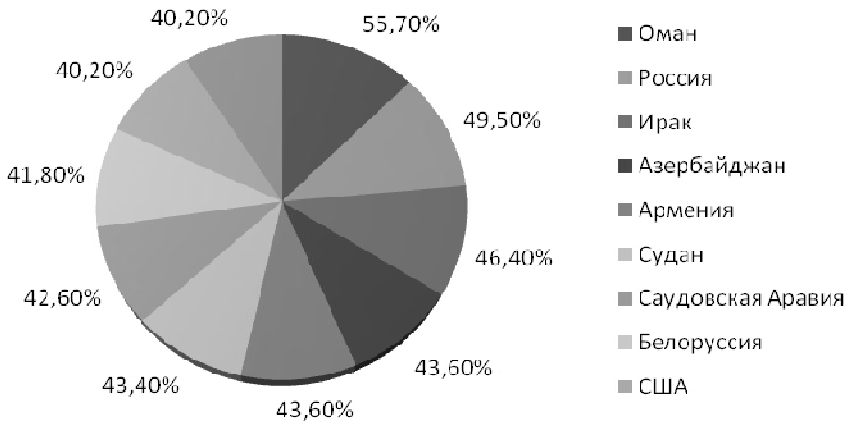

Рисунок 1 - Десять стран, где пользователи подвергаются наибольшему риску заражения через Интернет

Таким образом, проведенный анализ распределения вредоносных программ позволяет сделать вывод о том, что на сегодняшний момент ни одна организация не может обеспечить стопроцентную защиту информации, имеющейся у нее. Тем не менее, задача защиты информации от несанкционированного доступа должна стоять перед организацией на первом месте, необходимо постоянное совершенствование методов и способов обеспечения информационной безопасности экономических систем. В связи с этим, можно предложить следующий комплекс способов защиты информации:

- смарт-карты;
- биометрические системы;
- системы обнаружения вторжения (Intrusion Detection System, IDS);
- межсетевой экран.

Смарт-карты («smart» переводится, как интеллектуальная, умная) представляют собой пластиковые карты стандартного размера со встроенной электронной микросхемой, которая обычно состоит из микропроцессора, операционной системы, контролирующего устройства и кодированного доступа к данным его памяти. Применяется смарт-карта — в однофакторной или двухфакторной аутентификация пользователей, а также при хранении ключевой информации и проведении криптографических операций в доверенной среде. Они нашли свое применение, как носители документации - это студенческие билеты, удостоверения личности, водительские права, медицинские документы.

Биометрические системы состоят из двух частей - это оборудование и специализированное программное обеспечение. В состав оборудования входят сканеры и биометрические терминалы, а программное обеспечение, в свою очередь, эти данные обрабатывает, заносит информацию в базу данных и затем формирует отчетность для руководителей. Существует множество биометрических сканеров:

- отпечатки пальцев;
- голоса;
- конфигурации лица;
- отпечатки ладоней;
- узор радужной оболочки или сетчатки глаза;
- конфигурация руки;
- расположение кровеносных сосудов;
- динамика подписи;
- ритм работы на клавиатуре.

Все из перечисленных методов достаточно сложны, поэтому исключают попытки обмана.

Системы обнаружения вторжения (Intrusion Detection System, IDS) представляют собой устройства или

процессы, которые анализируют активность в сети и контролируют систему на предмет неавторизованных или несанкционированных действий. IDS предназначены для поимки злоумышленников на месте, прежде чем они нанесут действительно ущерб. Данная система также наблюдает за целостностью данных, сетевой активностью, проводит аудит системной и сетевой конфигурации.

На сегодняшний день из комплекса выделенных способов защиты информации наибольшее распространение получил межсетевой экран. Межсетевой экран (firewall,брандмауэр) - это устройство управления доступом, защищающее внутренние сети от внешних атак. Оно устанавливается на границе между внешней и внутренней сетью. Правильно сконфигурированный межсетевой экран является важнейшим устройством защиты. Однако он не сможет предотвратить атаку через разрешенный канал связи. Межсетевой экран подразделяется на экраны прикладного уровня и экраны с пакетной фильтрацией.

Межсетевые экраны прикладного уровня, или прокси-экраны, - это программные пакеты, которые основываются на операционных системах общего назначения (таких как Windows и Unix) или на аппаратной платформе межсетевых экранов. Прокси-экраны имеют несколько интерфейсов, по одному на каждую из сетей, к которым он подключен. Набор правил политики определяет, каким образом трафик передается из одной сети в другую. Если в правиле отсутствует явное разрешение на пропуск трафика, межсетевой экран отклоняет или аннулирует пакеты. Через межсетевой экран прикладного уровня проходят все соединения. Соединение берет начало на системе-клиент и попадает на внутренний интерфейс прокси-экрана, затем межсетевой экран принимает соединение, происходит анализ содержимого и протокол определяет, соответствует ли данный трафик правилам политики безопасности. Если все проходит успешно прокси-сервер инициирует новое соединение между внешним интерфейсом и системой-сервером

Межсетевой экран с пакетной фильтрацией также базируется на операционных системах (Windows и Unix), либо на аппаратных платформах межсетевых экранов. Он рассматривает каждый сетевой пакет отдельно от остальных и «не понимает» соединений. Отличие межсетевого экрана с пакетной фильтрацией от экрана прикладного уровня в том, что имее т возможность поддержки большего объема трафика, так как в нем отсутствует нагрузка, создаваемая дополнительными процедурами настройки и вычисления, имеющими место в программных модулях доступа [3].

При использовании межсетевого экрана с пакетной фильтрацией соединения не прерываются на межсетевом экране, а направляются непосредственно к конечной системе. При поступлении пакетов межсетевой экран выясняет, разрешен ли данный пакет, если это так пакет передается дальше по своему маршруту, в противном же случае пакет отклоняется или аннулируется.

Таким образом, проблему защиты информации сложно назвать надуманной. В современных условиях производство не может существовать и формироваться без высокоэффективной системы управления, основывающейся на информационных технологиях. Когда существенным ресурсом современной организации, способным в большей степени воздействовать на повышение его конкурентоспособности, инвестиционной привлекательности и капитализации, являются корпоративные информационные ресурсы и знания, которые нужно не только эффективно накапливать, но и обеспечивать безопасность.

Меры защиты необходимо блюсти во всех точках сети, при работе любых субъектов с информацией, где каждый информационный ресурс, будь то компьютер пользователя, сервер организации или сетевое оборудование, должны быть защищены соответствующим образом от всевозможных угроз. При этом обеспечить стопроцентную защиту невозможно, но вместе с тем нужно понимать, что чем выше уровень защищенности, тем эффективнее механизмы комплексной защиты предприятия. Однако самым уязвимым звеном в защите информации в современном мире является человек, ведь работоспособность любого программного обеспечения зависит от грамотности администратора, соответствующего средства защиты, от уровня дисциплинированности пользователей, которые работают с программным обеспечением.

Список литературы:

1. Блинов, А.М. Информационная безопасность учебное пособие [Текст] /А.М. Блинов. –СПб.: - Изд-во: СПбГУЭФ, 2010.-196 с.

2. Голдовский, И.С. Безопасность платежей в Интернете [Текст]/ И.С.Голдовский.- СПб.:Питер, 2011. -350с.

3. Конахович, Г. Ф. Защита информации в телекоммуникационных системах [Текст] /Г.Ф. Конахович.- Изд-во:МК-Пресс, 2011.-281 с.

4. Крошилин, С.В. Возможные угрозы безопасности экономических информационных систем и методы их устранения [Текст] / С.В. Крошилин //Проблемы и методы управления экономической безопасностью регионов: Материалы межвузовской научной конференции профессорско-преподавательского состава. - Коломна: КГПИ, 2010.- С.57-68.

5. Лукацкий, А.Н. Неизвестная VPN - Информзащита [Электронный ресурс]. - Режим доступа: http://www.infosec.ru/press/pub/p87.htm. Дата обращения 24.03.2012.

6. Парошин, А.А. Информационная безопасность: стандартизированные термины и понятия [Текст] /А.А. Парошин.- Изд-во ИНФРА-М, 2010.-216с.

7. Скородумов, Б.С. Обеспечение безопасности коммерческой информации в Интернет/интранет-сетях [Электронный ресурс]. - Режим доступа:http://www.bpc.ru/news/mirll-00.htm. Дата обращения 24.03.2012.

8. Скородумов, Б.С. Стандарты информационной безопасности - Институт экономической безопасности [Электронный ресурс] /Б.С. Скородумов, В.К. Иванов. - Режим доступа: http://www.bre.ru/business_news. Дата обращения 24.03.2012.

9. Шляхтина, С. В. Рынок ПО для обеспечения безопасности [Электронный ресурс] /С.В. Шляхтина. - Режим доступа:http://www.compress.ru/Archive/ Потенциальные ИТ-угрозы. Дата обращения 24.03.2012.

Звягинцева Юлия Александровна
к.э.н., доцент кафедры менеджмента
Орловского государственного института экономики и торговли
e-mai:yguliazv@yandex.ru

Павлова Юлия Николаевна
студентка 4 курса факультета управления,
Орловского государственного института экономики и торговли
e-mai:pavl_julia@mail.ru