В доступе отказано >>

Информационная безопасность: дань моде или жизненная необходимость

КАКОЙ УЩЕРБ БУДЕТ НАНЕСЕН ВАШЕМУ БИЗНЕСУ В СЛУЧАЕ УТЕЧКИ ИНФОРМАЦИИ? МОГУТ ЛИ МОШЕННИКИ ПОЛУЧИТЬ ДОСТУП К ВАШИМ СЧЕТАМ? СКОЛЬКО КЛИЕНТОВ ВЫ ПОТЕРЯЕТЕ, ЕСЛИ СПАМ И ВИРУСЫ ВЫВЕДУТ ИЗ СТРОЯ ИНФОРМАЦИОННУЮ СИСТЕМУ? НА ЭТИ И ДРУГИЕ ВОПРОСЫ ПОПЫТАЛИСЬ ОТВЕТИТЬ ЭКСПЕРТЫ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СОБРАВШИЕСЯ ЗА КРУГЛЫМ СТОЛОМ В РЕДАКЦИИ ЖУРНАЛА RM.

Приходится признать: несмотря на компьютеризацию практически всех бизнес-процессов на предприятии, не многие владельцы и топ-менеджеры уделяют должное внимание вопросу обеспечения информационной безопасности (ИБ). Интеллектуальная собственность, коммерческие и промышленные секреты, персональные данные клиентов – все это регулярно становится объектом хакерских атак. Нельзя исключать и риски возникновения программных сбоев, недостаточную квалификацию пользователей программного обеспечения, злой умысел сотрудников компании и т.д. Минимизировать последствия подобных событий призвана система управления информационной безопасностью (СУИБ).

Искандер Конеев: «Как правило, вместо полноценной системы обеспечения ИБ на предприятиях используются порой противоречащие друг другу разрозненные программные продукты, нормативные документы, практикуются неформальные взаимоотношения между сотрудниками и подразделениями. Необходимо понимать, что ИБ – это не набор внедренных технических решений, а сложная система, призванная обеспечить конфиденциальность, целостность и доступность информации. Это один из важнейших элементов поддержания непрерывности бизнеса. Не скрою, для построения эффективной СУИБ необходимы серьезные вложения, что может стать сдерживающим фактором для многих компаний».

Виктор Голубев: «Бизнес все сильнее зависит от надежности информационных систем. Но, к сожалению, далеко не всегда удается убедить руководство компании в необходимости и важности инвестиций в ИБ. На мой взгляд, мощными мобилизующими факторами повышения надежности информационных систем становятся сейчас требования внешних регулирующих законов, актов и стандартов, таких, например, как SOX, Basel II, ISO и др. Выход на IPO или проверка компании перед сделкой по слиянию могут послужить стимулом к усовершенствованию СУИБ».

Стандартные решения – не панацея

Информационная безопасность, пожалуй, одна из наиболее стандартизуемых сфер как с управленческой, так и с технологической точек зрения. Причем в последнее время наблюдается тенденция к унификации стандартов на международном уровне.

Виктор Сердюк: «Из российских нормативно-правовых документов по ИБ я бы обратил внимание на Федеральные

законы «Об информации, информационных технологиях и о защите информации», «О персональных данных», «О коммерческой тайне». Также существуют государственные и отраслевые стандарты (например, стандарт Банка России СТО БР ИББС 1.0) и другие специализированные документы, такие как требования ФСБ РФ и ФСТЭК (Федеральной службы по техническому и экспортному контролю)».

Александр Астахов: «Существует большое количество современных стандартов в области ИБ, разработанных международными организациями, – институтами, форумами и ассоциациями. Практически по каждому стандарту имеется богатый опыт применения, опробованные на практике руководства и методологии внедрения, а также интернет-ресурсы. Можно даже сказать, что стандартизация в данной области развивается быстрее, чем где бы то ни было. Постепенно современные стандарты будут адаптированы и для России. Определенное движение в этом направлении есть не только со стороны Банка России, но также со стороны ФСТЭК, ФАТРМ и других ведомств. Одной из приоритетных является задача скорейшей адаптации международных стандартов для русскоязычного сообщества».

Что делать и с чего начать

Искандер Конеев: «В соответствии с применяемыми сегодня стандартами ИБ – как западными, например, ISO 17799 и 27001, так и российскими, скажем, СТО БР ИББС 1.0-2006 – СУИБ строится на основе управления рисками. Но, не имея представления о ценности данных, которые могут быть утрачены, информационными рисками управлять невозможно. Однако иногда даже ключевые пользователи информационной системы затрудняются с оценкой ее значимости для компании.
Зачастую отчет, раскрывающий текущее состояние информационной системы и отражающий риски, которым она подвержена, может состоять из нескольких десятков или даже сотен страниц. При этом количество идентифицированных информационных рисков на крупном предприятии достигает иногда нескольких тысяч».

Андрей Зеренков: «Оценку IT-безопасности необходимо делать, обладая полным представлением обо всех аспектах функционирования информационных систем предприятия. А это означает, что начинать надо

>> В обсуждении приняли участие

Александр АСТАХОВ, *генеральный директор компании «ГлобалТраст Солюшинс»*

Виктор ГОЛУБЕВ, *директор департамента продаж IT-решений компании «IDS Scheer Россия и страны СНГ»*

Андрей ДРОЗДОВ, *старший менеджер отдела бизнес-консультирования аудиторской компании KPMG, CISM, CISA*

Андрей ЗЕРЕНКОВ, *руководитель службы консалтинга «Лаборатории Касперского»*

Искандер КОНЕВ, *менеджер Группы технологической интеграции компании Deloitte, CISSP*

Виктор СЕРДЮК, *генеральный директор компании «ДиалогНаука», канд. техн. наук*

Дмитрий ХАРЧЕНКО, *директор по маркетингу компании ElcomSoft Co. Ltd.**

** В настоящее время в компании Elcomsoft не работает. – Прим. ред.*

с IT-аудита, то есть сбора и структуризации информации обо всех имеющихся компьютерных ресурсах, используемом программном обеспечении и его конфигурации. Также необходимо классифицировать сведения по степени важности (или по стоимости потери/разглашения), определить системы и узлы, задействованные в создании, хранении и модификации информации, а также соответствующие документопотоки. Лишь после этого из общей IT-инфраструктуры можно вычленить участки, в первую очередь требующие оценки защищенности. И хотя от вредоносных программ и утечки данных следует защищать абсолютно все ресурсы (опыт показывает, что успешная атака на жизненно важные и серьезно охраняемые системы может быть проведена через незначительную брешь в защите второстепенного ресурса), оценить значимость всех выявленных рисков затруднительно. Это задача владельца информационного ресурса».

Андрей Дроздов: «В некоторых организациях требования по обеспечению ИБ не разработаны или неизвестны сотрудникам – механизм доведения информации о конфиденциальности отсутствует. Можно потратить много времени на построение безопасного периметра сети, установку межсетевых экранов и т.п., но если люди не имеют понятия о ценности информации, с которой они работают, все усилия могут оказаться тщетными».

Искандер Конеев: «Серьезная проблема заключается в отсутствии культуры управления ИБ в компании. Несмотря на то что уже несколько лет отраслевые стандарты и передовой опыт доказывают нам, что работы по управлению ИБ должны носить динамический или даже циклический характер, менеджмент продолжает воспринимать их как разовые мероприятия.
Усугубляют проблему и некоторые поставщики решений в области ИБ, позиционируя свой продукт или услугу как решение, которое сразу удовлетворит все потребности предприятия в этом ресурсе.
К сожалению, невозможно в рамках одного проекта внедрить СУИБ и обеспечить необходимый уровень защищенности на долгие годы. Разумнее продумать долгосрочную стратегию, когда СУИБ выстраивается в виде серии проектов по ИБ, а одновременно проводится подготовка сотрудников организации в плане соответствующей информационной культуры.
С перечисленными проблемами связан вопрос срока реализации проекта. Как я уже сказал, оптимальный вариант – это серия проектов. Сначала создается базовая структура СУИБ, потом предприятие привыкает к ней, затем производится уточнение отдельных направлений. Если предприятие действительно заинтересовано в развитии ИБ, то через 2–3 года, реализовав 3–4 проекта длительностью 2–4 месяца, мы можем говорить, что процесс работы СУИБ запущен

СПРАВКА

Где утечка?

Один из наиболее значимых рисков ИБ – утечка информации. По результатам исследования аналитического центра InfoWatch, **наибольшее количество утечек (50%) происходит с помощью мобильных устройств – ноутбуков, КПК, flash-накопителей.** Помимо очевидных преимуществ, компактность мобильных устройств является и не менее заметным недостатком с точки зрения защиты информации. Будь то ноутбук, КПК или флеш-карта, это устройство очень легко потерять или спрятать. Непреднамеренная утеря носителя информации приведет к тому, что конфиденциальные данные попадут к неизвестным лицам, которые распорядятся ими по своему усмотрению. В то же время внутренние нарушители легко могут спрятать маленький носитель и вынести данные с рабочего места.
Второй по распространенности канал утечек – это интернет (12%). Он не так популярен, поскольку не позволяет быстро передавать данные в объемах, доступных мобильным носителям. Кроме того, с помощью сетевой фильтрации достаточно легко найти источник утечки. Причиной 5% инцидентов послужили неправильно утилизованные или утерянные резервные носители, по 3% пришлось на электронную почту и факсы. 17% утечек внутренней информации происходит иными способами, например, в результате передачи бизнес-процессов на аутсорсинг. В 10% случаев выяснить, каким образом была украдена информация, не удалось.

и функционирует. Участие консультантов потребуется только в виде периодических аудитов ИБ, и это уже будут небольшие 2–3-недельные проекты».

Виктор Сердюк: «Можно назвать следующие общие меры для защиты информации:
- управленческие, предполагающие обеспечение правильной организации, взаимодействия и планирования подразделений компании для решения задач в области ИБ;
- операционные, направленные на реализацию функций обеспечения безопасности, выполняемых сотрудниками компании.

Выбор конкретных организационных или программно-технических мер защиты зависит от результатов оценки рисков ИБ.
Состав программно-технических мер защиты компании во многом зависит от специфики используемых информационных систем и тех задач, которые необходимо решать. Вместе с тем на сегодняшний день существует несколько ключевых подсистем, которые должны входить в состав комплекса защиты информации в компании:
- подсистема выявления компьютерных вирусов;
- подсистема обнаружения несанкционированных воздействий злоумышленников на сеть;
- подсистема анализа уязвимостей, позволяющих осуществить информационные атаки;
- подсистема персонального и межсетевого экранирования для блокирования опасных пакетов данных;
- подсистема контроля целостности для выявления последствий информационных атак;
- подсистема выявления спама;
- подсистема криптографической защиты информации (обеспечивает конфиденциальность и целостность передаваемых данных);
- подсистема защиты от угроз, связанных с утечкой конфиденциальных данных;
- подсистема мониторинга безопасности (выполняет функции централизованного сбора и анализа информации о событиях, связанных с угрозами)».

Виктор Голубев: «Практика показывает, что 90% всех операций, к какому бы департаменту они формально ни относились, прямо или косвенно касаются IT. Приведу характерный пример, связанный с управлением правами доступа к информационным системам одной компании. При приеме на работу сотрудника (или при расширении его полномочий) в скорейшей реализации запроса в IT-подразделении заинтересован линейный менеджер: ему нужно срочно ввести нового работника в строй. Обратная ситуация при увольнении: линейному менеджеру безразлично, удален ли увольняемый сотрудник из списков доступа к информационным системам или нет. За отсутствие в списках доступа фамилий уволенных сотрудников отвечает уже IT-отдел. Поэтому я и стал инициатором организации сквозного процесса в компании, охватывающего и бизнес-подразделения, и отдел кадров, и IT. Подписывая обходной лист уже после внедрения данного процесса, я был абсолютно уверен: если стоит подпись моего сисадмина, значит, увольняющийся сотрудник удален из всех информационных систем компании.
Еще более интересным опытом было распространение данной процедуры на наших многочисленных субконтракторов, использующих наши технологии и имеющих для этого доступ к нашим системам. Правда, для этого пришлось организовать сквозное взаимодействие уже не только внутренних бизнес-подразделений компании, но и внешних подрядчиков. На практике это вылилось в разработку, согласование и утверждение документов, регламентирующих порядок приема, перемещения и увольнения сотрудников у наших подрядчиков и, что особенно важно, порядок своевременного информирования нас об этих событиях».

Дмитрий Харченко: «Если аудит ИБ дает положительное заключение, это не должно стать поводом для ослабления внимания к информационной безопастности. Технологии постоянно развиваются: увеличивается мощность процессоров, разрабатываются новые методы. Пример: rainbow attack – это технология, которая быстро и легко взламывает многие из тех паролей, которые совсем недавно казались очень стойкими. Внутренние проверки должны проводиться сотрудниками отдела безопасности, которые подчиняются непосредственно руководству компании, и только ему. Желательно, чтобы сам факт проведения проверок не был известен остальным сотрудникам».

Есть ли перспективы?

В идеале меры по обеспечению ИБ должны опережать развитие угроз. Поэтому в стратегии управления безопасностью компании следует учесть необходимость повышения качества СУИБ и запланировать для этих целей соответствующие ресурсы.

СПРАВКА

Стандарты IT-безопасности

Международная организация по стандартизации (ISO) разработала ряд стандартов по внедрению СУИБ.
Стандарт ISO 17799 предназначен для всех организаций вне зависимости от сферы деятельности.
Стандарт ISO 27001 регламентирует проведение официальной сертификации СУИБ и описывает, в частности, следующие аспекты:

- политика безопасности;
- пользователи информационной системы;
- физическая безопасность;
- управление коммуникациями и процессами;
- контроль доступа;
- приобретение, разработка и сопровождение информационных систем.

Следует упомянуть и другие международные стандарты и рекомендации, получившие распространение в России:

- Стандарт CobiT (Control Objectives for Information and related Technology, «Контрольные объекты для информационной и смежных технологий»).
- Стандарт ITIL (Information Technologies Infrastructure Library, «Библиотека инфраструктуры информационных технологий»).
- OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation, «Методика оценки критических угроз, информационных активов и уязвимостей».

Александр Астахов: «В подавляющем большинстве российских компаний система управления рисками ИБ находится в зачаточном состоянии. Перечислим признаки такой ситуации.

1. Нет четкой определенной политики, методологии и процедуры управления рисками ИБ. Отсутствует реестр информационных рисков, на котором основаны декларация о применимости механизмов контроля и план обработки рисков. Как следствие, внутренние проверки ИБ проводятся хаотично и бессистемно, а выдаваемые рекомендации субъективны, фрагментарны и не имеют достаточного экономического обоснования. При этом вполне могут быть обнаружены как технические уязвимости, так и организационные недостатки в работе СУИБ предприятия. Однако отдельные и наиболее критичные информационные системы и бизнес-процессы могут полностью выпасть из поля зрения. А при таком подходе подсчитать возврат инвестиций в реализацию механизмов ИБ, оценить остаточные риски, определить уровень приемлемого риска и правильно обозначить приоритеты в сфере обеспечения ИБ не представляется возможным.
2. Руководство компании в своей политике ИБ четко не определяет стандарты, нормативные документы, законодательные и бизнес-требования, контрактные обязательства, которым организация должна следовать для обеспечения ИБ. В итоге нет конкретных утвержденных руководством критериев, в соответствии с которыми должно осуществляться управление рисками.
3. Руководство компании доверяет проведение анализа ИБ недостаточно подготовленным специалистам и отказывается инвестировать в их обучение и сертификацию. В такой динамично развивающейся области, как ИБ, человек, полгода нигде не обучавшийся, уже безнадежно отстает, и креатива от него ожидать сложно. При этом руководители рассуждают примерно так: «Мы взяли на работу высококвалифицированного специалиста. Если его профессиональной подготовки недостаточно для выполнения им своих обязанностей, тогда зачем мы платим ему такую высокую зарплату?» Многие руководители, будучи людьми старшего поколения, мыслят категориями безвозвратно ушедшего индустриального века, когда человек, получив однажды образование и специальность, пользовался этими знаниями на протяжении всей трудовой деятельности, с годами «наслаивая» на них свой собственный опыт. Их воспитание и образование не позволяют понять, что правила ведения бизнеса в новом информационном веке изменились».

Андрей Дроздов: «В продвинутых компаниях управление рисками ИБ осуществляется примерно следующим образом.

1. Департамент ИБ отвечает за разработку и внедрение политик, процедур безопасности, идентифицирует риски и угрозы в области ИБ, выполняет ряд специфических

АЛГОРИТМ

План мероприятий

Итак, чтобы обеспечить надежную защиту информации, необходимо провести ряд организационных и технических мероприятий, в том числе оценку информационной системы. Для этого проводится проверка имеющихся элементов защиты информации и внедрение недостающих. Информационные ресурсы следует классифицировать по типам, уровню секретности, местонахождению, форме представления данных и конкретным ответственным лицам.
Одновременно должна быть разработана политика ИБ (этот документ определяет цели в области ИБ, а также причины, по которым ИБ важна для организации).
В рамках этой работы составляются должностные инструкции для IT-персонала, обслуживающего информационную систему, с указанием ответственности за нарушения.
К нормативным документам по ИБ, за выполнение которых отвечают все сотрудники компании, относятся:
- соглашение о конфиденциальности;
- инструкция пользователя компьютерной сети, правила работы с паролями, внешними файлами и т.д.;
- положение о правах доступа к информационным ресурсам;
- положение об архивировании и восстановлении данных;
- порядок действий при возникновении нарушений правил.

Регламенты ИБ должны быть доведены до сведения ответственных сотрудников.

функций, таких как криптозащита, а также проводит мониторинг инцидентов ИБ (например, попыток вторжений в корпоративную сеть) ежедневно и даже в режиме онлайн.
2. Департамент информационных технологий (IT) отвечает за техническое внедрение и сопровождение информационных систем, а также за реализацию технических мер контроля безопасности в соответствии с требованиями департамента ИБ.
3. Департамент внутреннего аудита проводит периодические проверки выполнения требований корпоративных политик, регламентов и процедур, в том числе в области IT и ИБ. Например, распределяются ли права доступа в соответствии с утвержденными регламентами, осуществляется ли резервное копирование данных, происходит ли ознакомление пользователей с требованиями ИБ?
4. Департамент управления рисками обеспечивает общую методологию управления корпоративными рисками и взаимодействует с департаментом ИБ с целью интеграции рисков IT и ИБ в общую карту рисков организации».

Искандер Конеев: «В заключение отмечу необходимость более пристального внимания руководителей предприятий к вопросам ИБ. Скажем, общепринятой практикой работы любой организации считается наличие профессиональной охраны на входе в здание, хранение документов и наличных денег в сейфах, установка камер наблюдения и оконной сигнализации. Однако когда речь заходит об ИБ, необходимым средствам защиты уделяется порой меньше внимания, часто финансирование осуществляется по остаточному принципу. Между тем очевидно, что в условиях интеграции бизнеса и информационных технологий виртуальное пространство содержит огромное количество рисков. По оценкам экспертов, в ближайшие годы ИБ из внутренней опции предприятия превратится в серьезное конкурентное преимущество. Это логично, ведь клиенты доверяют компаниям как минимум информацию о себе, а как максимум – свои денежные средства. Естественно, что рост грамотности клиентов в вопросах ИБ заставит их из двух компаний с примерно равным уровнем предоставления услуг выбрать именно ту, где ИБ будет обеспечиваться наиболее полно. Руководителям российских предприятий не стоит пренебрегать этой тенденцией. Учитывая, что минимальный период для достижения качественного уровня ИБ занимает 2–3 года, необходимо соответствующим образом планировать развитие этого направления на своем предприятии». ■

Материал подготовила
Людмила Андреева